

K253SCH1

1 UNITED STATES DISTRICT COURT
2 SOUTHERN DISTRICT OF NEW YORK

3 UNITED STATES OF AMERICA,

4 v.

S2 17 Cr. 548 (PAC)

5 JOSHUA ADAM SCHULTE,

6 Defendant.

Trial

7 -----x
8 New York, N.Y.
9 February 5, 2020
10 9:00 a.m.

11 Before:

12 HON. PAUL A. CROTTY,

13 District Judge
14 and a jury

15 APPEARANCES

16 GEOFFREY S. BERMAN

17 United States Attorney for the
18 Southern District of New York

19 BY: MATTHEW J. LAROCHE

20 SIDHARDHA KAMARAJU

21 DAVID W. DENTON JR.

22 Assistant United States Attorneys

23 SABRINA P. SHROFF

24 JAMES M. BRANDEN

25 Attorneys for Defendant

-and-

DAVID E. PATTON

Federal Defenders of New York, Inc.

BY: EDWARD S. ZAS

Assistant Federal Defender

Also Present: Colleen Geier

Morgan Hurst, Paralegal Specialists

Achal Fernando-Peiris

John Lee, Paralegals

Daniel Hartenstine

Daniella Medel, CISOs, Department of Justice

K253SCH1

(In open court; jury not present)

THE COURT: Good morning. We're missing a couple of jurors.

MR. BRANDEN: We're missing a couple lawyers, too, but I think they're just in the restroom and they'll be right here, Judge.

THE COURT: Okay. Thank you.

THE DEPUTY CLERK: Missing one still, Judge. Ms. Thompson.

THE COURT: Is Ms. Shroff here?

MR. ZAS: She is, Judge. She may have just stepped out to go to the ladies' room.

THE COURT: Do you want to take up the letter dated February 4 about the production of a binder? Can you talk about that, Mr. Zas?

MR. ZAS: Your Honor, I apologize. It is out of my realm of expertise.

THE COURT: Okay. We'll wait then.

Ms. Shroff, I want to talk about the letter you sent last night about 3506-04.

MS. SHROFF: Okay, I'm sorry, your Honor. I had to run back down to the SCIF. I apologize for keeping you waiting.

THE COURT: All right. I have the letter. I understand the letter. Mr. Laroche or somebody from the

K253SCH1

1 government, why can't you produce the binder?

2 MR. LAROCHE: May I just have one moment with
3 Ms. Shroff. I just haven't seen the letter, I want to ask her
4 what the letter is.

5 (Counsel conferring)

6 MR. LAROCHE: We're going to make the binder
7 available, your Honor.

8 THE COURT: That takes care of that, Ms. Shroff.
9 Anything else you want to take up?

10 MS. SHROFF: Nice to have that power, Judge.

11 THE COURT: 302 kind of dictates that you get the
12 file, the binder as it was maintained at the time. Anything
13 else to take up?

14 MR. ZAS: Your Honor, I did want to take something up
15 with the Court, just on outstanding motions we don't think
16 we've received a ruling on. There was a motion we made by
17 letter dated January 17, it's the Smith v. Illinois issue about
18 our inability to do any investigation of the CIA witnesses.
19 And we moved for permission to conduct our usual background
20 investigation on the witnesses, or alternatively --

21 THE COURT: I thought we took care of this at the
22 final pretrial conference, Mr. Zas.

23 MR. ZAS: No, your Honor. I think at the final
24 pretrial conference you asked the government to respond by
25 letter, which they did. And that was the government's letter

K253SCH1

1 of January 24. We responded on January 27, and then we gave
2 the Court a list of outstanding issues, including this one. So
3 I just wanted to make sure we weren't waiving anything or the
4 issue didn't get lost in the shuffle. It may have.

5 THE COURT: All right. We'll take a look. The dates
6 of the -- give me the dates again.

7 MR. ZAS: The initial motion is a letter dated
8 January 17, 2020. The issue is mentioned again in a letter of
9 January 23. The government responded on January 24. We
10 replied to that on January 27.

11 THE COURT: We didn't take it up at the pretrial
12 conference? I have a vague recollection that you raised it
13 before.

14 MR. ZAS: I raised it.

15 THE COURT: And the government consented to a Google
16 search of the CIA witnesses.

17 MR. ZAS: That's right. We were advised that we had,
18 we were permitted to conduct a Google search or similar
19 Internet search of the witnesses' names, so long as we didn't
20 specifically tie the name to the agency. We then objected to
21 that, because we were then given guidance by Mr. Hartenstine
22 that that meant we could not, for example, put the name in with
23 important terms like WikiLeaks or spying or leaks or other
24 items like that.

25 So, our problem is, as we sit here today with the

K253SCH1

1 first CIA witness about to testify, we've literally been able
2 to do no investigation at all into this witness, or any of the
3 15 witnesses or so from the CIA. We're dependent entirely on
4 what the government has given us. So I commend them for giving
5 that to us but, we're supposed to have the right to do our own
6 independent investigation.

7 THE COURT: I'll take a look. Thank you.

8 MR. ZAS: Thank you, sir.

9 THE COURT: Mr. Laroche, do you want the witness on
10 the stand before the jury comes in?

11 MR. LAROCHE: That's fine, your Honor.

12 THE COURT: Okay. Do you want to bring in the
13 witness. Is the next witness in the witness room?

14 MR. LAROCHE: Yes, your Honor.

15 THE COURT: The second witness today?

16 MR. LAROCHE: Not yet, your Honor. But this witness
17 is going to be on for most, if not all, of the day.

18 THE COURT: Okay.

19 MR. LAROCHE: We will have that witness prepared to
20 come up if it looks like he is going to finish.

21 THE COURT: Thank you.

22 (Jury present)

23 THE COURT: Before we start, let me confirm with the
24 jury that all of you were successful in adhering to my
25 instructions last night that you not discuss the matter, and

K253SCH1

Weber - Direct

1 you avoid any research or investigation. Okay. Remember, the
2 case has to be decided based on the evidence that you hear in
3 this courtroom and only this courtroom and only the evidence
4 that you hear here.

5 Don't read any newspapers, don't watch any TV stories,
6 don't do any independent research. Pay attention to what
7 happens in the courtroom because that's what's going to define
8 your task when you begin your deliberations. All right.

9 David.

10 THE DEPUTY CLERK: Please state your name for the
11 record.

12 THE WITNESS: Jeremy Weber.

13 (Witness sworn)

14 THE COURT: Please sit down. Mr. Laroche.

15 MR. LAROCHE: Thank you, your Honor.

16 JEREMY WEBER,

17 called as a witness by the Government,

18 having been duly sworn, testified as follows:

19 DIRECT EXAMINATION

20 BY MR. LAROCHE:

21 Q. Good morning, Mr. Weber.

22 A. Good morning.

23 I don't have the sheet you had mentioned up here.

24 Q. Ah. Understood. We'll get you that sheet. Let's get
25 started first.

K253SCH1

Weber - Direct

1 Are you employed?

2 A. Yes, I am.

3 Q. Where do you work?

4 A. Central Intelligence Agency.

5 Q. How long have you worked at the Central Intelligence
6 Agency?

7 A. Coming up on 10 years now.

8 Q. Does that also go by the CIA?

9 A. Yes, it does.

10 Q. What is the CIA?

11 A. The CIA is one of the executive agencies, we are tasked
12 with collecting foreign intelligence.

13 Q. Prior to working at the CIA, where did you work?

14 A. I was active duty Marine Corps.

15 Q. How long were you in the Marines?

16 A. Almost six years.

17 Q. What were your roles in the Marines?

18 A. For the first half of my career in the Marine Corps, I was
19 a data systems specialist, an IT guy. And then after that, I
20 became a Marine security guard, guarding the embassies.

21 Q. I want to direct your attention to March 2017.

22 A. Yes.

23 Q. Were you employed by the CIA at that time?

24 A. Yes, I was.

25 Q. Are you familiar with a CIA group known as the Engineering

K253SCH1

Weber - Direct

1 Development Group?

2 A. Yes, I am.

3 Q. In 2017, were you working in that group?

4 A. Yes, I was.

5 Q. Does the Engineering Development Group also go by EDG?

6 A. Yes, it does.

7 Q. Today I am going to refer to that as EDG or group.

8 A. Okay.

9 Q. Generally, speaking what did that group do?

10 A. The EDG was tasked with creating cyber capabilities for use
11 in cyber operations.

12 Q. By cyber capabilities, did that include developing cyber
13 tools?

14 A. Yes, that would be correct.

15 Q. What is a cyber tool?

16 A. Cyber tool would be anything from a script to a program
17 that we created to collect information off of a computer
18 network.

19 Q. You said that those tools were also used in operations; is
20 that correct?

21 A. Yes, that's correct.

22 Q. What types of operations?

23 A. Cyber operations.

24 Q. Can you explain some of the targets of those operations,
25 without identifying them specifically?

K253SCH1

Weber - Direct

1 A. So, our targets typically fell into two categories.
2 Foreign governments, or non-nation state actors.

3 Q. What do you mean by non-nation state actors?

4 A. Terrorists, typically.

5 Q. I want to direct your attention to March 7 of 2017.

6 A. Okay.

7 Q. Were you working that day?

8 A. Yes, I was.

9 Q. Were you working at the CIA that day?

10 A. Yes, I was.

11 Q. On that day, did you learn about the public disclosure of
12 any of your group's work?

13 A. Yes, I did.

14 Q. Where was your group's work publicly disclosed?

15 A. It was disclosed on the internet, by WikiLeaks.

16 Q. Were there additional public disclosures of your group's
17 work by WikiLeaks?

18 A. Yes, there was.

19 Q. Approximately how many?

20 A. I don't know the specific number. I think it was around 20
21 or so, plus or minus.

22 MR. LAROCHE: Your Honor, may I approach?

23 THE COURT: Yes, you may.

24 Q. Mr. Weber, I just handed you what's been entered into
25 evidence as Government Exhibit 1. Do you recognize that?

K253SCH1

Weber - Direct

1 A. Yes, I do.

2 Q. How do you recognize it?

3 A. After reviewing the exhibit, I made a mark on it that I
4 would recognize.

5 Q. Does that exhibit contain the information that was
6 disclosed by WikiLeaks from your group?

7 A. Yes, it does.

8 Q. Was the information disclosed by WikiLeaks from your group
9 classified or unclassified?

10 A. It was mostly classified information.

11 Q. Where was that information stored within the group?

12 A. It was stored on our primary network called DevLAN.

13 Q. Is that a computer network?

14 A. Yes, it is.

15 Q. Is that computer network classified?

16 A. Yes, it is.

17 Q. Did everyone who worked in the group have access to all of
18 the information contained on Government Exhibit 1?

19 A. No.

20 Q. I want you to look around the courtroom. Do you see anyone
21 in the courtroom who worked in the group who had access to all
22 of the information on Government Exhibit 1?

23 A. Yes.

24 Q. Can you please identify where that person is sitting.

25 A. He's sitting at the table there, looks like wearing a black

K253SCH1

Weber - Direct

1 jacket.

2 MR. LAROCHE: Your Honor, let the record reflect that
3 the witness has identified the defendant.

4 THE COURT: Yes.

5 Q. How long have you known the defendant?

6 A. I knew him for the entirety of when I started at the
7 agency, until his departure from the agency.

8 Q. While the defendant worked at the CIA, how often did you
9 interact with him?

10 A. For most of the time, especially when he was a full-time
11 officer, I would say daily.

12 Q. Can you describe what your relationship was like with him.

13 A. We were close. I would consider him a friend. We worked
14 often together on projects. He was somebody that I looked to
15 all the time to collaborate with. We were close over all.

16 Q. Did there come a time when your relationship changed?

17 A. Yes.

18 Q. When approximately did it change?

19 A. It would have been late 2015, early 2016. Josh became
20 increasingly belligerent to another employee, and eventually I
21 had had enough of the situation, and no longer considered him a
22 friend.

23 Q. Are you aware of any time in which the defendant violated
24 CIA policy using the classified computer network used by your
25 group?

K253SCH1

Weber - Direct

1 A. Yes.

2 Q. When approximately did that happen?

3 A. April 2016.

4 Q. How do you know it happened?

5 A. I witnessed the modification in some log files that showed
6 that he modified some permissions, after explicitly being told
7 otherwise on how they should be set.

8 Q. How did he modify those permissions?

9 A. Josh was an administrator of the system, and he used those
10 administrative privileges to go against the orders of our
11 leadership.

12 Q. Was he authorized to do that?

13 A. No, he was not.

14 Q. What, if any, steps did you take as a result of those
15 actions?

16 A. I immediately informed management, and management had me
17 come in, I believe the following day, with some other system
18 administrators to remove his access to -- administrative access
19 to the system.

20 Q. What are some of the reasons you took those steps?

21 A. The main reason was we no longer trusted him to be an
22 administrator of the system. He had demonstrated that he was
23 willing to do things other than what was explicitly told to him
24 by his leadership.

25 Q. Why did you no longer trust him to be an administrator of

K253SCH1

Weber - Direct

1 the system?

2 A. The actions that he had taken to -- we had given him very
3 specific instructions on how, how things were going to be. And
4 the system was set up in such a way, following those
5 instructions, Josh went and changed it to the way he wanted it
6 to be, without informing anybody. And then, in addition to
7 that, like I said, his interactions with the other employee and
8 some statements he made about that employee were lies I felt.

9 Q. Did you view that as a problem?

10 A. Yes.

11 Q. Why?

12 A. The agency exists in a world of trust. We are granted
13 access to classified information, and we are trusted to only
14 use that information for the expressed reasons we're given
15 access to it. If you can't trust the person that you're
16 working with, you just aren't going to be able to do your daily
17 job.

18 Q. Why is that a problem if you can't trust that person?

19 A. If you can't trust that person, you can't, you're not going
20 to be able to work with them, because having access to some of
21 this classified information could lead to grave damage to the
22 U.S. government. If you can't share it with that person
23 anymore, that's -- you're effectively worthless at the CIA.

24 Q. Now, you said that Government Exhibit 1 contains the
25 group's work. Is that correct?

K253SCH1

Weber - Direct

1 A. Yes.

2 Q. Did the leaks come from any particular part of your group's
3 network?

4 A. Yes, it did.

5 Q. Which parts?

6 A. We had a product called Confluence, that was the data that
7 was initially disclosed on the March 7. And then another
8 product called Stash, later referred to as Bitbucket. It was
9 renamed. That's where the data came for the second set.

10 Q. So let's start with Confluence. When was the Confluence
11 information disclosed by WikiLeaks?

12 A. March 7.

13 Q. Approximately how much of Confluence was disclosed by
14 WikiLeaks during that first leak?

15 MS. SHROFF: Objection, your Honor, as to personal
16 knowledge from this witness on these issues.

17 THE COURT: Overruled.

18 Q. How much of Confluence was disclosed by WikiLeaks in the
19 initial leak?

20 A. It appeared to be everything up to a certain date.

21 Q. You said that the subsequent leaks also had information
22 from Stash?

23 A. That's correct.

24 Q. What types of things were disclosed from Stash?

25 A. The stuff that was disclosed from Stash was source code,

K253SCH1

Weber - Direct

1 user guides; things of that nature.

2 MR. LAROCHE: Ms. Hurst, can you please publish what's
3 been entered into evidence as Government Exhibit 13.

4 Q. Do you see Government Exhibit 13 on the screen in front of
5 you, Mr. Weber?

6 A. Yes, I do.

7 Q. Do you recognize this?

8 A. Yes, I do.

9 Q. What is it?

10 A. This is a user guide that we would often create to deliver
11 with our tools.

12 MR. LAROCHE: Ms. Hurst, can you please zoom in on the
13 top banner.

14 A. Yes.

15 Q. Mr. Weber, do you see that banner?

16 A. Yes, I do.

17 Q. Do you recognize it?

18 A. Yes, I do.

19 Q. What is it?

20 A. So this is a -- this is a banner that identifies both the
21 classification of the document, as well as dissemination
22 controls for said document.

23 Q. Which portion of this is the classification?

24 A. The first half.

25 Q. And that's the "secret;" is that correct?

K253SCH1

Weber - Direct

1 A. Correct.

2 Q. And you said the other part has dissemination control?

3 A. That's correct.

4 Q. What do you mean by dissemination control?

5 A. So, in this scenario, "noforn" means no foreigners. This
6 would -- this says who we could share the document with. You
7 might have a scenario where this says "Rel To" and a country
8 name. Which means we're willing to share this information with
9 a specific country.

10 MR. LAROCHE: Could we zoom out again, Ms. Hurst.

11 Q. Mr. Weber, was this one of the Stash documents that was
12 disclosed by WikiLeaks?

13 A. That is correct.

14 MR. LAROCHE: Could we, Ms. Hurst, can we please zoom
15 in on the logo at the top.

16 Q. Do you recognize this logo?

17 A. Yes.

18 Q. What is it?

19 A. This is logo for the Information Operations Center.

20 Q. What is the Information Operations Center?

21 A. The Information Operations Center is a portion of the
22 agency that's tasked with conducting cyber operations for the
23 agency.

24 Q. I know you talked about the group which we've called EDG.
25 Was EDG within that operations center?

K253SCH1

Weber - Direct

1 A. Yes, it was.

2 MR. LAROCHE: Ms. Hurst, can you please zoom out. And
3 zoom in on the title below the logo, please.

4 Q. Is this a reference to your group?

5 A. Yes, it is.

6 Q. You see the U next to it on the left?

7 MS. SHROFF: Your Honor, could we have a sidebar for a
8 minute please?

9 THE COURT: What's the problem.

10 MS. SHROFF: I can't see my screen.

11 THE COURT: I'll see you at the sidebar.

12 (Continued on next page)

K253SCH1

Weber - Direct

1 (At the sidebar)

2 THE COURT: What's the problem?

3 MS. SHROFF: I can't see my screen. Unbeknownst to
4 me, behind my back, somebody's put a screen protector on it. I
5 don't know why.

6 MR. LAROCHE: The government did not put a screen
7 protector on it. We have no objection to removing the screen
8 protector.

9 MS. SHROFF: Mr. Kamaraju's screen doesn't have a
10 screen protector.

11 THE COURT: Listen, apparently it was put on there not
12 on the government's intent. Do you want it off?

13 MS. SHROFF: I do want it off.

14 THE COURT: David, how long will it take to take the
15 screen protector off?

16 THE DEPUTY CLERK: It takes seconds.

17 (Continued on next page)

K253SCH1

Weber - Direct

1 (In open court)

2 THE COURT: Has the problem been corrected?

3 MS. SHROFF: Yes, it has.

4 THE COURT: Thank you. Mr. Laroche.

5 Q. The last question I asked was about the U on the left of
6 this title here. What does that designate?

7 A. That's what we refer to as a portion mark. This sentence
8 is a non-classified sentence. So the U is to help with
9 identifying that.

10 Q. If we can just zoom out again. What is the top
11 classification of this document?

12 A. Secret.

13 Q. How do you know that?

14 A. So, the classification banner at the top, we are told and
15 we're trained that the classification contains the highest
16 level of information that's within the document. So, in this
17 case it would have been secret.

18 MR. LAROCHE: Ms. Hurst, can you please zoom in on
19 lines that start Brutal Kangaroo and the next three lines below
20 that.

21 Q. Are you familiar with Brutal Kangaroo?

22 A. Yes, I am.

23 Q. How are you familiar with it?

24 A. I advised Josh while he was writing it. I don't think I
25 contributed anything of significance to this specific project.

K253SCH1

Weber - Direct

1 But Brutal Kangaroo was also a successor to a tool that I had
2 created.

3 Q. Is Brutal Kangaroo a cyber tool?

4 A. Yes, it is.

5 Q. Who developed Brutal Kangaroo?

6 A. Primarily Josh Schulte.

7 Q. Under Brutal Kangaroo there's Drifting Deadline?

8 A. Yes.

9 Q. What is Drifting Deadline?

10 A. Drifting Deadline was a specific component of the Brutal
11 Kangaroo tool suite.

12 Q. What do you mean a component of the tool suite?

13 A. Brutal Kangaroo was meant to be a wide-ranging tool that
14 would be used in multiple scenarios. So, it had different
15 pieces to do different things on the network.

16 Q. And the bottom line of this says "user guide"?

17 A. Yes.

18 Q. What's a user guide?

19 A. A user guide is something developers would create so that
20 our mission partners would know how to use the tool, what the
21 risks of using the tool are, and things like that.

22 Q. You used the word mission partners. What do you mean by
23 mission partners?

24 A. Mission partner is the official term for our customers.

25 The people, we would make the tools and they would be used by

K253SCH1

Weber - Direct

1 another group. Those are our mission partners.

2 Q. Were those mission partners using the tools against foreign
3 or domestic targets?

4 A. Foreign targets.

5 MR. LAROCHE: If we can zoom out again, please. Go to
6 page four of this document.

7 Q. Do you recognize this page?

8 A. This appears to be page one still.

9 Q. Sorry. Page four of the PDF. Page one of the document.
10 Do you recognize this page?

11 A. Yes.

12 MR. LAROCHE: Zoom in, Ms. Hurst, from scope --
13 perfect.

14 Q. Could you read the scope.

15 A. "This document establishes the user guide for Drifting
16 Deadline version 1.2."

17 Q. And then also below 1.1, can you read the first sentence.

18 A. "Brutal Kangaroo is a tool suite for targeting closed
19 networks by air gap jumping using thumb drives."

20 Q. Just what is that portion marking?

21 A. That is an S for secret.

22 Q. Why is it secret?

23 A. This is getting into the methods of how the tool works,
24 which would have been considered secret.

25 Q. The first sentence refers to the tool suite that you

K253SCH1

Weber - Direct

1 referenced earlier; is that correct?

2 A. Yes.

3 Q. Then it says "targeting closed networks."

4 A. That's correct.

5 Q. What does that mean?

6 A. A closed network is a network that has limited connection
7 to other networks. Typically, when we are referring to a
8 closed network, we are saying a network that is not connected
9 to the internet.

10 Q. Then next part says "targeting closed networks by air gap
11 jumping." What does air gap jumping mean?

12 A. Air gap jumping was a trade craft term that we used. That
13 referenced getting data off of a network without a network
14 connection.

15 Q. Can you please read the second sentence.

16 A. "Brutal Kangaroo components create a custom covert network
17 within the targeted closed network and provide functionality
18 for executing surveys, directory listings, and arbitrary
19 executables."

20 Q. Can you summarize what that's saying?

21 A. Brutal Kangaroo would -- created a custom file system on
22 the thumb drives it was using to carry commands between
23 machines on the network.

24 So in this specifically, they're talking about saying
25 what type of computer surveys you would want, so this could be

K253SCH1

Weber - Direct

1 anything from what files are on a computer to what software is
2 installed on the computer. Directory listings is one of those
3 surveys I just talked about. And then arbitrary executables
4 would be secondary payloads that we might deploy on the system.

5 Q. What do you mean by secondary payloads?

6 A. So, often this would be additional tools to do other things
7 on the network, beyond just file collection.

8 Q. Give us an example.

9 A. Usually, the best example would be a back door, so that we
10 would have future access to the system.

11 MR. LAROCHE: Ms. Hurst, can you please go to page
12 six, and zoom in on the paragraph that starts the first tab to
13 the bottom, the rest of the page.

14 Q. Mr. Weber, do you see that paragraph starting first tab?

15 A. Yes.

16 Q. Can you summarize what that's addressing.

17 A. So, these are the different execution vectors that Drifting
18 Deadlines would use to gain execution, which that's, that is
19 the official term for starting the program. So, sometimes the
20 scenario would be a user would start the program for us,
21 sometimes it would be what's referred to as an exploit to gain
22 execution. The EZCheese link files and the Lachesis link files
23 would be the exploits.

24 Q. Are you familiar with the term attribution?

25 A. Yes, I am.

K253SCH1

Weber - Direct

1 Q. What does it mean?

2 A. Attribution is the identification of, it's tying an
3 activity to an actor. In our scenario, it would be somebody
4 catching CIA tools in the wild and then being able to say we
5 know this is the CIA, because of these reasons. That's
6 attribution.

7 Q. Is attribution to the CIA problematic for your work?

8 A. Yes, it is.

9 Q. Why?

10 A. So, we operate in secrecy. Foreign governments do not want
11 us on their networks, and would complain, to put it lightly, if
12 they caught us doing this. So, there is a wide gulf between
13 having a tool caught, and then having information in there
14 where a foreign government could publicly say the CIA was
15 hacking us, the U.S. government is not being a good player.

16 Q. What, if any, impact did the disclosure of this have on
17 attribution of this tool?

18 A. So --

19 MS. SHROFF: Objection.

20 THE COURT: Overruled.

21 A. These -- the information that is listed here would be clues
22 to attribution. So if Brutal Kangaroo or Drifting Deadlines
23 was caught on a foreign system somewhere, it might have been
24 sitting on somebody's desk, they knew this would be malware.
25 They wouldn't know necessarily whose malware it was. Seeing a

K253SCH1

Weber - Direct

1 document like this would allow them to start building a case
2 against the U.S. government saying, no, this was -- this was a
3 CIA tool that was used on our system.

4 Q. What, if any, impact would that attribution have on the use
5 of these terms in the future?

6 A. If we were concerned about the attribution of a tool to the
7 CIA, we would stop using it.

8 MR. LAROCHE: Ms. Hurst, you can pull that down.

9 Q. Mr. Weber, I just showed you one document that's contained
10 on Government Exhibit 1. Is that correct?

11 A. Yes.

12 Q. Approximately how many documents were disclosed by
13 WikiLeaks in Government Exhibit 1?

14 A. I don't know the exact number, but it would be thousands.
15 More than hundreds. It took a team of -- I was on a team of
16 about 10 people. It took us about a week of very long days to
17 just go through the initial disclosure.

18 Q. Generally, what impact did the public disclosure of your
19 group's information have on CIA's work?

20 A. It was crippling. We -- we were shut down for a
21 significant amount of time. There was a significant amount of
22 review about the operations that were ongoing to see what risk
23 there was. And we had to recreate a significant number of
24 capabilities.

25 Q. Why was there risk to operations?

K253SCH1

Weber - Direct

1 A. It goes back to both the attribution piece as well as the
2 information that was disclosed in WikiLeaks could be used by
3 the defensive community to potentially identify and find out
4 malware on foreign systems.

5 Q. What do you mean by malware?

6 A. Malware is the -- the industry term for cyber tools. I'm
7 sorry.

8 Q. We're going to come back to the leak later. I want to
9 switch gears just a little.

10 You said you started at the CIA, you've been at the
11 CIA for about 10 years?

12 A. That's correct.

13 Q. Are you familiar with the phrase "security clearance"?

14 A. Yes.

15 Q. What is a security clearance?

16 A. Security clearance is the U.S. government's trust in us as
17 individuals to have access to classified information.

18 Q. Do CIA employees need a security clearance to work there?

19 A. Yes, they do.

20 Q. Are there different levels of security clearance?

21 A. Yes, there are.

22 Q. What level?

23 A. There are three levels: Confidential, secret, and top
24 secret.

25 Q. Can you describe some of the differences between those

K253SCH1

Weber - Direct

1 levels.

2 A. The difference in levels means the level of information
3 that you would have access to, and it is graded by the amount
4 of potential damage that could be done to the U.S. government.
5 Confidential information, the official term is it would cause
6 damage. Secret level, the official term is serious damage.
7 And top secret is grave damage.

8 Q. What level security clearance do you need to work within
9 the group?

10 A. Top secret.

11 Q. When did you first obtain your security clearance?

12 A. I first obtained a security clearance shortly after joining
13 the Marine Corps.

14 Q. How do you obtain one?

15 A. At that time, it was a secret clearance, which involved me
16 filling out a lot of paperwork that explained everything from
17 where I've lived, who my friends were, who my family was, what
18 my financial status was. So you would submit this paperwork,
19 and then it's followed up by a background investigation where I
20 would talk with an investigator essentially about the paperwork
21 I had submitted.

22 Q. When you started at the agency, the CIA, did you obtain
23 your top secret clearance?

24 A. I had obtained a top secret clearance prior to the CIA.

25 Q. When you started with the CIA, were you required to take an

K253SCH1

Weber - Direct

1 oath?

2 A. Yes, I was.

3 Q. Can you explain what oath you were required to take.

4 A. We take an oath to support and defend the Constitution of
5 the United States.

6 Q. Where did you take that oath?

7 A. The oath is taken at the headquarters building of the CIA
8 on the CIA's seal in the front lobby.

9 Q. Does that seal have any significance to the CIA?

10 A. That seal along with -- there's a memorial right next to
11 the seal, it has a significant amount of significance. It's
12 meant to represent everything that we are doing.

13 Q. Are all employees required to take that oath before they
14 work at the CIA?

15 A. All staff employees.

16 Q. Let's talk for a moment about the structure of your group.
17 The Engineering Development Group.

18 A. Okay.

19 MR. LAROCHE: Ms. Hurst, can you please publish to the
20 witness, the parties and the Court what's marked as Government
21 Exhibit 89.

22 Q. Do you see Government Exhibit 89 on your screen, Mr. Weber?

23 A. Yes, I do.

24 Q. What is it?

25 A. This is a portion of the org chart for CCI, the portion

K253SCH1

Weber - Direct

1 that EDG was.

2 Q. Does this exhibit fairly and accurately represent that
3 portion of the org chart as it existed in 2015 and 2016?

4 A. Yes, it does.

5 MR. LAROCHE: The government would offer Government
6 Exhibit 89 into evidence.

7 MS. SHROFF: No objection, your Honor.

8 THE COURT: 89 is in evidence.

9 (Government's Exhibit 89 received in evidence)

10 MR. LAROCHE: Ms. Hurst, can you please publish it for
11 the jury.

12 Q. Mr. Weber, can we just start at the top. You referenced
13 Center for Cyber Intelligence?

14 A. Yes.

15 Q. Where does that appear on this exhibit?

16 A. That's at the top here. CCI.

17 Q. What is CCI?

18 A. CCI -- I forget when exactly, it was a few years ago. We
19 referenced IOC earlier. CCI was IOC renamed.

20 Q. IOC was the Information Operations Center; is that correct?

21 A. Yes.

22 Q. That was renamed as CCI?

23 A. That's correct.

24 Q. Below CCI there is a box for Engineering Development Group.
25 Is that correct?

K253SCH1

Weber - Direct

1 A. Yes.

2 Q. Is that the group you've been talking about today?

3 A. Yes.

4 Q. Below EDG, your group, what appears next?

5 A. Applied Engineering Division.

6 Q. Does that also go by AED?

7 A. Yes, it does.

8 Q. What is AED?

9 A. AED was a division in EDG. Our primary job was to create
10 cyber tools for the group. We were in-house developers.

11 Q. What do you mean by in-house developers?

12 A. So, we worked in the same building that our mission
13 partners worked in. The cyber operations are extremely
14 tailored. It involves a lot of back and forth with our mission
15 partners. So the in-house developers were closely tied into
16 the operations so we can create the best capability possible.

17 Q. Below AED are five boxes. What do each those boxes
18 reflect?

19 A. The different branches within AED.

20 Q. How many developers work within each of those branches?

21 A. Roughly, usually between 10 and 20 developers, depending on
22 the branch.

23 Q. Focusing on the branch at the left, the Operations Support
24 Branch. Are you familiar with that branch?

25 A. Yes.

K253SCH1

Weber - Direct

1 Q. How are you familiar with it?

2 A. I spent approximately six years as a developer within OSB.

3 Q. Approximately what time frame?

4 A. From when I was hired all the way until 2016.

5 Q. Did the defendant also work in that branch?

6 A. Sorry, correction. It's 2017 is when I stopped working
7 there.

8 And yes, the defendant did work in that branch.

9 Q. From approximately when?

10 A. The -- from the -- even before he was hired full-time, he
11 was an intern in OSB. And then for almost the entirety of his
12 career he was in OSB.

13 Q. What was the purpose of that branch, OSB?

14 A. OSB was focused on what we referred to as physical access
15 operations.

16 Q. What is that?

17 A. Physical access operation is a scenario where we, the
18 agency, had the capability to effectively touch a computer, be
19 it through an agency officer or an agency asset.

20 Q. What do you mean by touch a computer?

21 A. It could be anything. It could be somebody who was willing
22 to type on a keyboard for us. It often was somebody who was
23 willing to plug a thumb drive into the machine. Or it could be
24 a scenario where somebody was willing to literally pick a
25 machine up and walk off with it.

K253SCH1

Weber - Direct

1 Q. You used the word "asset" a second ago.

2 A. Yes.

3 Q. What were you referring to?

4 A. An asset is a term in the CIA for a -- for a foreigner who
5 has been recruited to work for the CIA.

6 Q. What was the culture of OSB like when you worked there?

7 A. We were very mission focused. We, we work closely with
8 each other. We got along with each other. We were, I would
9 say, mostly friends. It was, the -- working at the agency, you
10 always kind of have the finish line in your sights and the
11 exact mission that you're working on, and that's what drives
12 us.

13 Q. What do you mean by mission?

14 A. So, our mission is to, again, it's to support and defend
15 the Constitution. So, we are tasked with getting information
16 to policy makers so that they can effectively chart the
17 direction the United States should go.

18 Q. Did OSB have a professional atmosphere while you were
19 there?

20 A. It was mostly professional. I would say no more or less
21 professional than any other software development shop.

22 Q. What do you mean by that?

23 A. You know, again, our primary focus was on the mission.
24 But, you know, we had fun at work, too. We would occasionally
25 poke fun at each other. We were all friends.

K253SCH1

Weber - Direct

1 Q. How often did you interact with the defendant while he was
2 in the branch?

3 A. I would say daily.

4 Q. Generally, what were those interactions like?

5 A. I, I considered him a friend. Again, I worked closely with
6 him. I liked working with him. Josh, you know, I would say
7 mostly positive, although Josh, Josh sometimes would exhaust
8 you a little bit in those interactions.

9 Q. What do you mean by that?

10 A. You know, Josh was very opinionated on the way things
11 should be done. And wasn't somebody that could often be swayed
12 of said opinion. So, he had some rough edges that you would
13 have to deal with. You kind of took the good with the bad.

14 Q. Did you observe the defendant interact with other
15 developers in the branch?

16 A. Yes.

17 Q. What were those interactions like?

18 A. Mostly positive outside of one developer. I think most
19 developers within the branch would have the same opinion.

20 MS. SHROFF: Objection as to what opinion anyone else
21 had.

22 THE COURT: Yes. Sustained.

23 Q. You said one, as to one developer there was a different
24 relationship; is that correct?

25 A. Yes.

K253SCH1

Weber - Direct

1 Q. What was that developer's name?

2 A. Amol.

3 Q. We'll come back to Amol and the defendant later.

4 Looking back at the chart that's in front of you.

5 A. Okay.

6 Q. The top of the chart has CCI; is that correct?

7 A. That's correct.

8 Q. While you worked within CCI, where was it physically
9 located?

10 A. CCI was in an office building that was west of Washington,
11 D.C.

12 Q. Just going to refer to that as the CCI building or the
13 office. Okay?

14 A. Okay.

15 Q. Was anyone free to walk into that office?

16 A. No.

17 Q. What stopped them?

18 A. There was a fence around the entire compound, and to get
19 past that fence and enter the compound, you had to get past
20 armed security.

21 Q. How was that security armed?

22 A. Military grade weapons.

23 Q. How did you get past that security?

24 A. To get past that security, you had to present your
25 identification. For full-time employees, that would be your

K253SCH1

Weber - Direct

1 I.C. badge, and then they would let you on to the compound.

2 Q. You said I.C. badge. What's the I.C. stand for?

3 A. Intelligence community.

4 Q. Is the CIA part of the intelligence community?

5 A. Yes, it is.

6 Q. Once you got through the armed guards, could you just walk
7 into the office building?

8 A. No.

9 Q. What stopped you?

10 A. There were -- the way I would typically go in, were what we
11 referred to as full-height turnstiles. To get past those, you
12 would need to, you would need to badge in, which would be, you
13 would tap your badge against like a receiver. And then you
14 would have to put in a private code. The other way that you
15 could go in were also turnstiles that had armed security by
16 them.

17 Q. Could you hop over those turnstiles?

18 A. The ones with the armed security, you could hop over, I
19 would not recommend it. The turnstiles that I typically went
20 through there was no way to hop over. It was essentially a
21 wall.

22 Q. Did the CIA store classified information at this office?

23 A. Yes, it did.

24 Q. Generally speaking, in what kinds of places did it store
25 that classified information?

K253SCH1

Weber - Direct

1 A. What we referred to as a SCIF. A secure compartmented
2 information facility. It is, it is a large vault.

3 Q. What do you mean by that?

4 A. So, SCIFs have very strict rules on how they are set up,
5 access controls, things like that. They have heavy metal doors
6 that the first person that comes in for day has to put in a
7 combination to unlock the door. And then anybody after that
8 would have to badge in to gain access to the room.

9 Q. Were there any restrictions on what you could bring into
10 that office building?

11 A. Yes, significant.

12 Q. What types of restrictions?

13 A. There's, pretty much any personal electronics were not
14 allowed. Weapons, photography equipment, cell phones. When
15 you come into any agency building, there's always a sign that
16 says these are the prohibited items. It is a pretty lengthy
17 sign.

18 Q. Why are you not permitted to bring electronic devices into
19 the office?

20 A. They would introduce a risk to the classified information
21 that's stored there.

22 Q. What do you mean by that?

23 A. The best example would be if you brought in a cell phone.
24 You, an adversary might be able to leverage that cell phone to
25 listen to conversations that were ongoing in there. Or

K253SCH1

Weber - Direct

1 something like that.

2 Q. When you badged into the building through the turnstiles,
3 were you in a SCIF?

4 A. No.

5 Q. Where were the SCIFs located within the building?

6 A. They -- they were all -- they were all individual rooms
7 that you had to enter after badging through.

8 MR. LAROCHE: Your Honor, with the Court's permission,
9 I'd like to read a stipulation.

10 THE COURT: Yes.

11 MR. LAROCHE: It is hereby stipulated and agreed by
12 and among the United States of America by Geoffrey S. Berman,
13 United States Attorney for the Southern District of New York,
14 David W. Denton, Jr., Sidhardha Kamaraju, and Matthew Laroche,
15 Assistant United States Attorneys, of counsel, and Joshua Adam
16 Schulte, the defendant, by and with the consent of his counsel,
17 Sabrina Shroff, Esq., Edward Zas, Esq., and James Branden,
18 Esq., that:

19 Government Exhibit 100 is a compact disc containing
20 true and accurate CIA badge records for (i) Joshua Adam Schulte
21 identified as Government Exhibits 105, 107, 108 and 109; (ii)
22 Rufus, identified as Government Exhibits 101 and 112; (iii)
23 David, identified as Government Exhibits 102 and 113; (iv)
24 Timothy identified as Government Exhibits 103 and 114; (v)
25 Andrew identified as Government Exhibit 104; (vi) Jeremy Weber

K253SCH1

Weber - Direct

1 identified as Government Exhibits 106 and 117; (vii) Michael
2 identified as Government Exhibit 115; and (viii) Amol
3 identified as Government Exhibit 116. Government Exhibits 101
4 through 109 and 112 through 117 were made at or near the time
5 by, or from information transmitted by, a person with knowledge
6 of the matters set forth in the records; they were kept in the
7 course of the regularly conducted business activity; and it was
8 the regular practice of that business activity to maintain the
9 records. The time stamps on Government Exhibits 101 through
10 109 and 112 through 117 reflect local time in 24-hour format.

11 Government Exhibit 111 is a true and accurate copy of
12 floor plans for the eighth and ninth floor for the CIA's Center
13 for Cyber Intelligence office in which the defendant worked.

14 Government Exhibit 200 is a compact disc containing
15 true and correct copies of portions of the defendant's CIA
16 personnel file, including Government Exhibit 201, which is a
17 training the defendant took while employed at the CIA;
18 Government Exhibit 202, which is a portion of the defendant's
19 CIA employee bio; government Exhibits 401 through 405, which is
20 various non-disclosure agreements and security paperwork signed
21 by the defendant prior to resigning from the CIA; Government
22 Exhibits 406 and 408, which are various of the defendant's
23 performance activity reports at the CIA; Government Exhibit 409
24 is a letter of warning provided to the defendant on or about
25 June 22, 2016; and Government Exhibit 411 is a complaint filed

K253SCH1

Weber - Direct

1 by the defendant to the Office of Equal Employment Opportunity
2 Commission.

3 Government Exhibit 300 is a compact disc containing
4 true and accurate copies of documents marked as Government
5 Exhibits 301 through 304, recovered from the defendant's desk
6 area following his resignation from the CIA.

7 Government Exhibit 500 is a compact disc containing
8 true and correct copies of portions of the defendant's CIA
9 security file, including Government Exhibits 506 through 507,
10 which are outside activities reports completed by the defendant
11 while employed at the CIA; Government Exhibit 505, which is a
12 complainant statement signed by the defendant while employed at
13 the CIA; Government Exhibit 508 is excerpts of a recording of
14 an April 8, 2016, interview of the defendant while at the CIA;
15 and Government Exhibit 509 is excerpts of a recording of a
16 July 19, 2016 interview of the defendant while at the CIA.

17 Government Exhibits 601 through 616 are true and
18 accurate copies of network documentation for certain CIA
19 computer systems.

20 Government Exhibits 701, 702, 704 through 708, 712
21 through 714, 716, 718, 719 and 720 are true and accurate copies
22 of electronic communications that were transmitted over CIA
23 messaging systems. The time stamps on the foregoing exhibits
24 reflect local time in 24-hour format.

25 And Government Exhibits 1001 through 1012, 1015

K253SCH1

Weber - Direct

1 through 1056, 1058 through 1098, 1100 through 1103, 1105, 1107,
2 1108, 1110 through 1116, 1118, 19, 21, 24, 1128 through 1130000
3 are true and accurate copies of e-mail communications sent and
4 received using CIA computer systems.

5 And finally, Government Exhibit 5001 is a true and
6 accurate copy of portions of the CIA's October 17, 2017
7 WikiLeaks Task Force Final Report.

8 It is further stipulated and agreed that this
9 stipulation, Government Exhibit 3004, and all of the exhibits
10 identified in this stipulation, may be received in evidence as
11 government exhibits at trial.

12 THE COURT: They're received in evidence.

13 MR. LAROCHE: Thank you, your Honor.

14 (Government's Exhibit 3004, 100, 111, 200, 300, 500
15 received in evidence)

16 (Government's Exhibit 601-616, 701, 702, 704-708
17 received in evidence)

18 (Government's Exhibit 712-714, 716, 718, 719, 720
19 received in evidence)

20 (Government's Exhibit 1001-1012, 1015-1056, 1058-1098
21 received in evidence)

22 (Government's Exhibit 1100-1103, 1105, 1107, 1108
23 received in evidence)

24 (Government's Exhibit 1110-1116, 1118, 1119, 1121
25 received in evidence)

K253SCH1

Weber - Direct

1 (Government's Exhibit 1124, 1128-1130, 1132-1137, 5001
2 received in evidence)

3 MR. LAROCHE: Ms. Hurst, can you please publish what's
4 marked as Government Exhibit 1011. Sorry. 111. And go to the
5 second page of this exhibit.

6 Q. Mr. Weber, do you recognize this?

7 A. Yes, I do.

8 Q. What is this?

9 A. This is a floor plan for the ninth floor of our office
10 building.

11 Q. Just to orient us a bit, was OSB located on the ninth floor
12 as of 2015 and 2016?

13 A. Yes, it was.

14 MR. LAROCHE: Ms. Hurst, can you just zoom in on the
15 middle portion of this. Right in the middle of the document.

16 Q. Just in the middle there, Mr. Weber, what are we looking
17 at?

18 A. The middle is the elevators to get to the ninth floor.

19 Q. Can you just circle on the screen where the elevators are.

20 A. So this was the primary bank of elevators. And then this
21 one over here is a freight elevator.

22 Q. The portions you just circled, is that within a SCIF area?

23 A. No, it is not.

24 Q. We can zoom back out, please.

25 MS. SHROFF: Mr. Laroche, are we looking at the

K253SCH1

Weber - Direct

1 circling?

2 MR. BRANDEN: The circle is not showing up.

3 THE DEPUTY CLERK: Mr. Laroche, I think now it's
4 working.

5 MR. LAROCHE: Thank you, David.

6 Q. If we could clear the screen, please.

7 THE COURT: The yellow circle is the elevators and the
8 purple circle is the freight elevators?

9 THE WITNESS: I don't know where the yellow line came
10 from, your Honor. The larger circle is the regular elevators.
11 And actually, the circles that were just shown were off.

12 MR. LAROCHE: Maybe we could zoom in again so we can
13 have the record clear for everyone.

14 Q. Can you please just circle, once this is zoomed in, the
15 elevators again, please. Thank you.

16 A. Yes. So, these are the regular use elevators, and then
17 this right here is a freight elevator.

18 MR. LAROCHE: If we can zoom out again, please.

19 Q. Mr. Weber, can you please circle where OSB sat as of 2015
20 and 2016.

21 A. Yes. That would be this area right over here.

22 MR. LAROCHE: Can we zoom in on that area, please,
23 Ms. Hurst.

24 Q. Can you circle that area again where OSB sat.

25 A. Yes. This area.

K253SCH1

Weber - Direct

1 Q. I think OSB appears on this zoomed in version. Could you
2 just circle it?

3 A. Yes.

4 Q. What do these reflect? I know they're a little blurry.

5 A. The area that I circled would have been cubicles.

6 Q. Is this area within a SCIF?

7 A. Yes, it is.

8 Q. How do you get into this SCIF?

9 A. There were multiple entrances to this SCIF, but it was all
10 through, again, you would badge into the SCIF through one of
11 the many doors.

12 Q. As of 2015, can you circle where you sat within OSB?

13 A. Yes.

14 Q. What about the defendant?

15 MR. LAROCHE: Thank you. We can pull that exhibit
16 down.

17 Q. We've been talking about the office that CCI worked in.

18 A. Yes.

19 Q. Were you allowed take classified information out of that
20 building?

21 A. Only with specific authorization.

22 Q. How would you obtain that authorization?

23 A. You would request it. There was a form you would, or like
24 a web page you would go to, to say what you were taking, where
25 you were taking it to, and what the purpose was for traveling

K253SCH1

Weber - Direct

1 with classified information.

2 Q. Were you allowed to take classified information home?

3 A. No.

4 Q. Why not?

5 A. Your home is not a secure place to store classified
6 information.

7 Q. Was there any procedure in place if you did take classified
8 information to a place you weren't supposed to?

9 A. Yes, there was.

10 Q. Can you describe that procedure.

11 A. If you mistakenly took classified information to a location
12 you weren't supposed to, you were instructed to immediately
13 return to whatever closest facility there was, and then report
14 to both the agency security officer as well as your leadership.

15 Q. Did you ever have to follow that procedure?

16 A. Yes, I did.

17 Q. Can you explain what happened?

18 A. So, early in my career, it was tax time. We are, we are
19 sent our tax documents electronically. I printed off the tax
20 documents which are unclassified, but, whenever you print
21 something, you have what is referred to as a cover page. And
22 that cover page says treat this information as classified. I
23 accidentally brought that cover page home one day.

24 Q. Can you describe what that cover page looks like?

25 A. It just has your user name and says the information

K253SCH1

Weber - Direct

1 following this might contain classified information. And that
2 it was U.S. government.

3 Q. What did you do with the cover page after you found it at
4 home?

5 A. Brought it back into work.

6 Q. What happened as a result of that?

7 A. I reported it to management and the ASO, but there was no
8 further action. They told me not to do it again.

9 Q. Did you use a classified e-mail system at the CIA?

10 A. Yes, I did.

11 Q. Did you ever send unclassified e-mails on that system?

12 A. Yes, I did.

13 Q. Why would you do that?

14 A. The -- the classification of an e-mail has nothing to do
15 with the system that it's on. It is the information that's
16 contained in that e-mail. So, an unclassified e-mail might be
17 something as simple as, let's meet at, you know, 3 p.m. in this
18 room number. Nothing in there is damaging to the U.S.
19 government. That would be an unclassified e-mail.

20 Q. How would you notify someone if you were sending an
21 unclassified e-mail?

22 A. Every single e-mail that we sent, you were required to
23 classify before sending it. So, the e-mail would carry a
24 classification banner as well as a classification block.

25 Q. Just want to show you one example.

K253SCH1

Weber - Direct

1 MR. LAROCHE: Ms. Hurst, if we can publish Government
2 Exhibit 1023. If we can go to the second page of this exhibit.
3 Just zoom in on the to from line here.

4 Q. Do you recognize this to be a CIA e-mail?

5 A. Yes, I do.

6 Q. Who sent this e-mail?

7 A. This would have been sent by Joshua Schulte.

8 Q. When did he send it?

9 A. January 6, 2016, at 3:06 p.m.

10 Q. Who did he send it to?

11 A. Rufus.

12 Q. Did he copy anyone on the e-mail?

13 A. He copied myself and Sean.

14 Q. What was the subject of this e-mail?

15 A. "Migration of Atlassian servers and support back to ISB."

16 MR. LAROCHE: If we can zoom from classification down.

17 Q. Just starting at the top of the screen, there is a
18 classification secret/nofor with a cross through. What does
19 that reflect?

20 A. So, this would have been the overall classification of the
21 e-mail.

22 Q. Who classified the e-mail?

23 A. The e-mail is classified by the sender, so in this case
24 Josh.

25 Q. How would the sender classify the e-mail?

K253SCH1

Weber - Direct

1 A. There was a tool tied into our e-mail system that you would
2 select what the classification was, as well as what reason you
3 were classifying the document.

4 Q. Okay. We'll come back to the substance of this e-mail
5 later.

6 MR. LAROCHE: Ms. Hurst, you can pull that down.
7 Thank you.

8 Q. You stated and you talked a little bit about the
9 development of cyber tools by the group.

10 A. Yes.

11 Q. Generally speaking -- strike that.

12 Who tasked you to create cyber tools?

13 A. Our mission partners would.

14 Q. Who were your mission partners?

15 A. In -- typically, it's COG, which was another group within
16 CCI. Like I mentioned earlier, EDG made the tools, COG would
17 deploy them in operations.

18 Q. What does COG stand for?

19 A. Computer Operations Group.

20 Q. After you were tasked to create a cyber tool, how would you
21 go about creating it?

22 A. So, there was significant back and forth when you are
23 creating a tool. You would interact closely with COG to make
24 sure you were creating the right thing. Once you understood
25 the mission parameters, the AED, we would write the source code

K253SCH1

Weber - Direct

1 that would eventually in turn create the capability.

2 Q. You used the term "source code."

3 A. Yes.

4 Q. What is source code?

5 A. So, source code is what software developers create. It is
6 human readable computer instructions that eventually will be
7 compiled into a computer readable program.

8 Q. How did you go about developing source code?

9 A. We would write it. This is what we're trained to do.

10 Q. Are you familiar with a cyber tool called Marble or
11 Marbler?

12 A. Yes, I am.

13 Q. Generally speaking, what does that tool do?

14 A. It was an internal tool, meant -- it was used by developers
15 in AED to aid in the development of capabilities. Its job was
16 to, one of our pieces of trade craft was to obfuscate strings
17 which could be identifying information in a binary. So,
18 Marbler would obfuscate the strings for us.

19 Q. You used the term "trade craft." What does that mean?

20 A. Trade craft is the lessons learned, the rules, everything
21 like -- you're taught how to be a software developer in
22 college. The agency then takes that raw material and trains
23 you on how to be somebody who creates cyber tools. The trade
24 craft is the training that you get for this is how you, you
25 know, do X, Y and Z. These are best practices, things like

K253SCH1

Weber - Direct

1 that.

2 MR. LAROCHE: Ms. Hurst, can you please publish
3 Government Exhibit 12-2.

4 Q. Mr. Weber, do you recognize this?

5 A. Yes, I do.

6 Q. What is it?

7 A. This is source code.

8 Q. Was this source code disclosed by WikiLeaks?

9 A. Yes, it was.

10 Q. What is this source code for?

11 A. This was a portion of Marbler.

12 Q. How do you recognize this to be source code?

13 A. I wrote stuff very similar to this. This is C++ code which
14 is a computer language. And a lot of the words and things in
15 here are what are referred to as key words. So, anybody who is
16 a C++ developer would recognize this.

17 Q. So I want to go to one page of this and see if you can help
18 us understand it. If we go to page five. Then if we can just
19 zoom in on the top all the way down to "go to reset." That's
20 fine. Just want to focus you on the middle where it starts
21 "generate modified files."

22 Do you see that?

23 A. Yes.

24 Q. Could you summarize what that's saying.

25 A. So, this is generate modified files is a function call.

K253SCH1

Weber - Direct

1 So, this is the -- what's done in generate modified files is
2 defined elsewhere in the source. But, this function is called,
3 and then immediately after this function, we check to see if
4 there was any error during the running of this. And if there
5 was an error, we print to the user that there was a problem and
6 that you're resetting the files before proceeding on.

7 Q. What do you mean by print to the user?

8 A. So, Marbler was what we referred to as a command line tool.
9 Think your old DOS prompt where you've got just text on the
10 screen. So, this would, this would write to that screen error
11 in modifying files resetting to original files.

12 Q. Is this source code classified?

13 A. Yes, it is.

14 Q. Why?

15 A. The techniques in here are part of our trade craft. And
16 having access to this information and the tie to the CIA would
17 help an adversary with the attribution aspect of the
18 identification.

19 MR. LAROCHE: Ms. Hurst, we can pull that down.

20 Q. When source code is complete for a tool that you're
21 developing, what happens to it?

22 A. It's, in the case of C++, it's compiled, which is a tool
23 that is used to convert that human readable files into machine
24 readable code.

25 Q. What is that machine readable code then called?

K253SCH1

Weber - Direct

1 A. We typically refer to that as a binary or a program.

2 Q. Why do you create binary from the source code?

3 A. So, in compiled languages, computers can't execute source
4 code. So, it doesn't understand, it doesn't understand the
5 documents that we write, so it's converted to a language the
6 computer understands.

7 Q. Other than the source code and the binary, do developers
8 create any documentation for their cyber tools?

9 A. Yes.

10 Q. What are some of the types of documentation they create?

11 A. The main type of documentation you would see would be a
12 user guide, which explains how to use the tool, why you would
13 use the tool, and what scenarios you would use the tool. We
14 also were a bureaucracy at heart, so there would also be
15 delivery records with everything that we did and there would be
16 a paper trail. We would help in the creation of those
17 documents as well.

18 Q. When the source code, the binary and those documents are
19 complete, what happens to the tool?

20 A. We, it would go through what we referred to as the delivery
21 process. That information would be handed over to our SIs,
22 system integrators, who would then take it to the configuration
23 management team who would store the information, as well as
24 hand it over to COG so that they could use the tool.

25 Q. Earlier in your testimony you talked about a computer

K253SCH1

Weber - Direct

1 network that was used by the group; is that correct?

2 A. Yes.

3 Q. From which the information on Government Exhibit 1 came
4 from. Is that right?

5 A. Yes.

6 Q. I want to focus you on 2015 and 2016.

7 A. Okay.

8 Q. Was that computer network used to develop cyber tools?

9 A. Yes, it was.

10 Q. What was that computer network called?

11 A. DevLAN.

12 Q. What does DevLAN mean?

13 A. It was, it was abbreviation for dev, which short for
14 development, and LAN was short for local area network. So, it
15 was just a shortened term to reference that.

16 Q. What's local area network mean?

17 A. Local area network is an industry term for a network that
18 is controlled by a company or something like that.

19 Q. Were you familiar with the DevLAN network?

20 A. Portions of it.

21 Q. How did you become familiar with portions of that network?

22 A. One, my day-to-day job was leveraging the resources that
23 were on DevLAN. And secondly, I was an administrator for a
24 portion of the network.

25 Q. What do you mean by administrator?

K253SCH1

Weber - Direct

1 A. I had additional privileges on some of the services that
2 were run on the network, to ensure that those services stayed
3 up and running, granting access to who needed access to those
4 services, things like that.

5 Q. Did any other developers share in those administrative
6 privileges?

7 A. Yes.

8 Q. Who?

9 A. At the time you referenced, it would have been Joshua
10 Schulte. Just before that, it would have been Patrick.

11 Q. Who is Patrick?

12 A. Patrick was a developer within AED as well. He originally
13 brought the Atlassian products in house and helped set them up.
14 But he was selected for a new assignment, and passed those
15 responsibilities off to me.

16 Q. What was the classification level of the DevLAN network?

17 A. Top secret.

18 Q. Why did it have that classification level?

19 A. The information that was on the network would often be up
20 to top secret in nature.

21 Q. Was DevLAN connected to any unclassified network?

22 A. No, it was not.

23 Q. Was DevLAN connected to the internet?

24 A. No, it was not.

25 Q. Why not?

K253SCH1

Weber - Direct

1 A. Being connected to the internet would pose a serious risk
2 to the security of that network. It would give essentially the
3 adversaries a front door into accessing it.

4 Q. I'd like to focus on how the DevLAN network was set up or
5 its infrastructure. Generally speaking, what is network
6 infrastructure?

7 A. Network infrastructure is anything that's needed for a
8 computer network to run. Generally speaking, you've got three
9 categories of stuff. The end user's machines, think the laptop
10 or desktop that you would use on a daily basis. The servers,
11 which are powerful machines that sit in the back that contain a
12 lot of the information. And then intermediary devices on the
13 network whose job is to transfer the data back and forth.

14 Q. Are you familiar with the term "closed network"?

15 A. Yes, I am.

16 Q. What is a closed network?

17 A. A closed network is a network that has limited access, if
18 any access to other networks. And traditionally speaking, when
19 we refer to a closed network, we are saying it is a network
20 that is not connected to the internet.

21 Q. Was DevLAN a closed network?

22 A. Yes, it was.

23 Q. Why was it a closed network?

24 A. It was a top secret network, which meant that there were,
25 there was a lot of security procedures that we had to follow.

K253SCH1

Weber - Direct

1 And one of the easier ways to defend a network is by making
2 sure that it does not have access to the internet.

3 MR. LAROCHE: Ms. Hurst, can you please publish to the
4 Court, the parties, and the witness what's marked as Government
5 Exhibit 1251.

6 Q. Mr. Weber, do you recognize this?

7 A. Yes, I do.

8 Q. What is it?

9 A. It is a high level, it is a high-level view of portions of
10 DevLAN, as well as COG's network and Hickok.

11 Q. Does it fairly and accurately represent those portions of
12 the network you just described and in about 2015 and 2016?

13 A. Yes, it does.

14 MR. LAROCHE: The government offers 1251 into
15 evidence.

16 MS. SHROFF: Your Honor, we have an objection.

17 THE COURT: You have no objection?

18 MS. SHROFF: We do have an objection.

19 THE COURT: It's overruled.

20 MR. LAROCHE: Can we publish that for the jury?

21 THE COURT: 1251 is received in evidence.

22 (Government's Exhibit 1251 received in evidence)

23 MR. LAROCHE: Thank you, your Honor.

24 Q. There is a lot on this screen. We're going to walk through
25 it, Mr. Weber. First, did DevLAN run computer software?

K253SCH1

Weber - Direct

1 A. Yes, it did.

2 Q. Are you familiar with the term Atlassian?

3 A. Yes, I am.

4 Q. What is Atlassian?

5 A. Atlassian is a commercial company that creates products for
6 software development.

7 Q. Did DevLAN include certain Atlassian services?

8 A. Yes, it did.

9 Q. What services?

10 A. There were five of them: Confluence, Bamboo, Crowd, Jira,
11 and at the time, it was called Stash, that product has been now
12 renamed to Bitbucket.

13 Q. If we can focus on the top left. You see some of the
14 Atlassian services here?

15 A. Yes.

16 Q. Can we circle Confluence, please. What is Confluence?

17 A. Confluence is a product for generating or presenting
18 user-generated content. It's similar to something like
19 Wikipedia where multiple users can edit the same page, and it's
20 a collaborative work environment.

21 Q. Can you please circle Bamboo on the screen. This is
22 another one of the Atlassian services run on DevLAN?

23 A. Yes, it is.

24 Q. What did Bamboo do?

25 A. Bamboo, to use an industry term, was used for continuous

K253SCH1

Weber - Direct

1 integration. Which meant whenever source code was changed,
2 Bamboo would detect that change, compile the code, and test the
3 code. It was meant to make it so that if you introduced an
4 error in your code, you discovered it early and can correct it
5 right away.

6 MR. LAROCHE: Ms. Hurst, if you can zoom out, please.
7 Then zoom in on the box with the Stash server.

8 Q. Can you please circle Stash on this. What was Stash?

9 A. Stash was meant to, to back up the source code that we
10 wrote on a daily basis, as well as provide an area for us to
11 collaborate and discuss that source code.

12 Q. Can you please circle Crowd. What did Crowd do?

13 A. Crowd's job was to translate the user permissions that
14 were -- like the user authentication was handled by an external
15 service called Active Directory. So, all of the user
16 authentication, things like that, would be handled by Active
17 Directory. Crowd's job was to interface with Active Directory
18 and then let the Atlassian products know who an authorized user
19 was and what groups they belonged to.

20 MR. LAROCHE: Just zoom out one more time, please.
21 Zoom in on the box with Hickok.

22 Q. What is Jira?

23 A. Jira is a tool for issue tracking. Which, that's
24 everything that we need to do when we are developing a tool.
25 It could be anything from the background of this web page needs

K253SCH1

Weber - Direct

1 to be blue and not green, to something like in this scenario,
2 the program crashes, and we need to fix this. Jira was meant
3 to track all of those work items. So that you can report the
4 status of how far you've progressed in your development.

5 Q. If we can zoom out again, please. Did DevLAN also have
6 hardware?

7 A. Yes, it did.

8 Q. What types of hardware did it have?

9 A. It had, all, all types of hardware. For the most part, the
10 users had desktops as their work machines. It had computer
11 servers. It had switches, routers, everything that you would
12 find on a traditional network.

13 Q. Let's focus on the servers.

14 MR. LAROCHE: Ms. Hurst, if you can zoom in on the top
15 left, the ESXi server.

16 Q. What is an ESXi server?

17 A. ESXi is another commercial tool that its job is to -- it's
18 referred to as a hypervisor. It's meant to enable running what
19 we refer to as virtual machines. It allows you to run multiple
20 virtual machines on a single set of hardware. Something like
21 that.

22 Q. In 2015, what branch did the ESXi server belong to?

23 A. This specific one belonged to OSB.

24 Q. What programs were being run on that ESXi server?

25 A. It was running a Confluence virtual machine, a Bamboo

K253SCH1

Weber - Direct

1 virtual machine, as well as a collection of development VMs for
2 different purposes.

3 Q. You used the term "virtual machine."

4 A. Yes.

5 Q. Is that the same thing as a VM?

6 A. Yes.

7 Q. What is a virtual machine?

8 A. A virtual machine is technology that we use in the IT
9 world. It is a way to try and separate the operating system
10 and any services from the hardware it's running on.

11 Hardware ages and eventually fails. So, virtual
12 machines are supposed to make it so that you're agnostic to the
13 hardware you're running on. So when a server begins to fail,
14 you can quickly migrate that service to something new.

15 Q. What's the purpose of that?

16 A. It's, in the IT world, you are pretty much judged based
17 solely on what we refer to as uptime, meaning, is a user able
18 to use the service that you're responsible for. So, having a
19 server fail would cause significant impact on your uptime. And
20 this is a way of just making sure that that wouldn't happen.

21 MR. LAROCHE: Ms. Hurst, can you please zoom out then
22 zoom in on the Stash server.

23 Q. Was there a separate server that was running Stash?

24 A. That's correct.

25 Q. Can you explain that?

K253SCH1

Weber - Direct

1 A. Stash, the server was owned and operated by ISB. Stash was
2 not a virtual machine, because there is a cost to running
3 virtual machines. It's not as efficient as running on a
4 straight hardware. And we wanted to make sure Stash, which was
5 the most used of the services, had enough power to, you know,
6 meet the division's needs.

7 Q. You used the term ISB.

8 A. Yes.

9 Q. What is ISB?

10 A. ISB was the branch within EDG whose focus was on system
11 administration of DevLAN.

12 Q. What does ISB stand for?

13 A. Infrastructure Support Branch.

14 MR. LAROCHE: Ms. Hurst, can you please zoom out. Can
15 we please publish again Government Exhibit 111.

16 Q. You just talked about the OSB's ESXi server. Is that
17 correct?

18 A. Yes.

19 Q. And a Stash server?

20 A. Yes.

21 Q. Where were those located?

22 A. They were located in server rooms.

23 Q. On what floor?

24 A. The ninth floor.

25 Q. Let's start with the OSB ESXi server.

K253SCH1

Weber - Direct

1 A. Okay.

2 Q. Do you see the server room in which the OSB ESXi server was
3 located as of 2015 and 2016?

4 A. Yes, I do.

5 Q. Can you please circle that server room.

6 A. This one right here.

7 Q. Is that server room within a vault?

8 A. Yes, it is.

9 Q. Can you please circle the server room in which the Stash
10 server was located in 2015 and 2016.

11 A. That would be this one right here.

12 Q. Who did that server room belong to?

13 A. ISB.

14 Q. Thank you.

15 MR. LAROCHE: We can take that down, please.

16 Q. You stated that COG, the Computer Operations Group, used
17 the tools that were developed by some of the branches within
18 EDG; is that right?

19 A. That's correct.

20 Q. Did COG users have their own computer network?

21 A. Yes, they did.

22 Q. I am going to refer to as the COG network.

23 MR. LAROCHE: Ms. Hurst, can you please publish
24 Government Exhibit 1251 again.

25 Q. Did COG users have access to the cyber tools on DevLAN?

K253SCH1

Weber - Direct

1 A. Not directly, no.

2 Q. What do you mean by that?

3 A. Any tools that we created on DevLAN would be delivered to
4 COG, usually by CD, and then stored on COG's network.

5 Q. Did COG users have access to Confluence on DevLAN?

6 A. No, they did not.

7 Q. Did COG users have access to any of the Atlassian services?

8 A. Yes, they did.

9 Q. Which one?

10 A. Jira.

11 Q. How did COG users have access to Jira?

12 A. Jira existed on an intermediary network in between DevLAN
13 and COG called Hickok.

14 Q. Could COG users access other Atlassian services through
15 Hickok?

16 A. No.

17 Q. How do you know that?

18 A. COG users did not have credentials to DevLAN. And all of
19 the other Atlassian products would require DevLAN credentials.
20 And also, COG users, there wasn't a network, direct network
21 connection that they could travel over.

22 MR. LAROCHE: We can pull that down for a second,
23 Ms. Hurst.

24 Q. Let's talk for a moment about how the Atlassian services
25 were backed up.

K253SCH1

Weber - Direct

1 A. Okay.

2 Q. Are you familiar with the term "data backup"?

3 A. Yes, I am.

4 Q. What does that mean?

5 A. So, the data we created on DevLAN was our day-to-day work.
6 Losing that would mean that we would have to recreate it and
7 would take a significant amount of time.

8 To defend against this, you would create a data
9 backup, which was a copy of the data done usually daily or
10 something of that frequency. So that if there was an incident,
11 disaster, something like that, we could get back without losing
12 much work.

13 Q. Focusing on 2015, were the Atlassian services backed up?

14 A. Yes, they were.

15 Q. How?

16 A. So, in 2015, the data backups were to the -- originally to
17 the local drives that they were -- the local machines that they
18 existed on. So Confluence wrote to the Confluence machine,
19 Stash back up its data to the Stash machine.

20 MR. LAROCHE: Ms. Hurst, can you please publish
21 Government Exhibit 1251 again. Just zoom in on the ESXi server
22 for a moment.

23 Q. Can you explain what you mean by there being a time where
24 the backups were stored on the machines themselves?

25 A. Yes. So, in this case, Confluence, all of the data that

K253SCH1

Weber - Direct

1 was generated, was on Confluence VM. So on a hard drive that
2 belonged to Confluence. The backups would write to the same
3 hard drive, just a different folder location.

4 Q. Was that problematic?

5 A. Very.

6 Q. Why?

7 A. Two reasons. One, the backups took up a significant amount
8 of space. And it caused a problems with Stash, where one day
9 Stash would no longer turn on, because we literally used up
10 every, every bit of hard drive space for that machine.

11 But more importantly, a backup to the local machine is
12 just a bad idea. Because most likely, your reason for needing
13 a backup is the computer that the service was running on
14 failed. And so your backup failed in that scenario too.

15 Q. Did there come a time when the backups were not stored
16 locally?

17 A. Yes.

18 Q. Where were they stored after that?

19 A. They were stored on a NetApp on DevLAN. And then to an
20 offsite location as well.

21 MR. LAROCHE: Ms. Hurst, can you zoom out for a
22 second. Then zoom in on the middle bottom box, the NetApp
23 server.

24 Q. Is this the NetApp you were referring to?

25 A. Yes.

K253SCH1

Weber - Direct

1 Q. What is a NetApp server, generally?

2 A. NetApp is another commercial technology. They are focused
3 on what is referred to as network attached storage, which is
4 meant to be file systems that are accessed over a network
5 drive.

6 (Continued on next page)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

K25Wsch2

Weber - Direct

1 BY MR. LAROCHE:

2 Q. Where were the backups stored on NetApp?

3 A. There was a folder created on the NetApp called Altabackup.

4 Q. How often were the Atlassian services backed up to the
5 Altabackup?

6 A. I believe it was daily.

7 Q. How were the data backups moved to the Altabackup from the
8 Atlassian services?

9 A. So, when Altabackup was created, each of the Atlassian
10 products was modified as well as the VMs or machines they were
11 running on. The Altabackup folder was what we refer to as
12 mounted in the Linux drive, so for general purposes, that
13 meant -- it looked like any other folder on your system.

14 Q. Were the backups stored within any other location other
15 than the Altabackup?

16 A. Yes.

17 Q. Where?

18 A. They were in an offsite location also in the WMA area.

19 Q. Other than the Alta backups, was there anything else stored
20 on the NetApp server?

21 A. Yes, there was.

22 Q. What else was stored on the NetApp server?

23 A. A significant amount of information. Some examples would
24 be users' home directories, which, for every DevLAN user, they
25 would get a folder on the NetApp that they controlled who had

K25Wsch2

Weber - Direct

1 access to what on that folder. And then there was also just a
2 general file share, so if we had software that we had
3 downloaded or something like that, it could be stored there.

4 Q. Are you familiar with the term Gold source copies?

5 A. Yes, I am.

6 Q. What are those?

7 A. When we would finish a tool and deliver it to COG, there
8 would be an official record made. So the final version of the
9 binary that we were delivering, any documentation and any
10 source code would be given to the configuration management
11 team, and that information would then be stored as an official
12 record.

13 Q. Did you store the information in the Gold source copies?

14 A. No, I did not.

15 Q. Why not?

16 A. That wasn't my job, and I don't believe I had access to
17 that folder.

18 Q. Generally speaking, who had access to the DevLAN network?

19 A. Users in EDG.

20 Q. As of 2015 and 2016, approximately how many people had
21 DevLAN access?

22 A. Probably around a hundred, give or take. It was almost
23 exclusively AED, so the -- most of the -- all of the developers
24 and then a few other individuals.

25 Q. How did users access DevLAN?

K25Wsch2

Weber - Direct

1 A. So, when you -- when you join the group, you would check in
2 with ISB. ISB would create a user name and password for you,
3 in Active Directory, and those credentials, which were unique
4 to you, were leverage to access those resources on DevLAN.

5 Q. Did individual users have their own DevLAN computers?

6 A. Yes, they did.

7 Q. Where were those computers located?

8 A. Typically, at the desk that they worked at on a daily
9 basis.

10 Q. Were those desks within the vaults you described earlier?

11 A. Yes.

12 MR. LAROCHE: Ms. Hurst, can you zoom out on 1251,
13 please.

14 Q. Are the DevLAN users reflected on this diagram?

15 A. Yes.

16 Q. Where are they?

17 A. Right over here.

18 Q. Is that the bottom left corner of 1251?

19 A. Yes. Sorry.

20 Q. How were users' accesses controlled?

21 A. The main way was through Active Directory permissions.
22 Again, you would be given an Active Directory username and
23 password, and your account would be assigned to different
24 Active Directory groups.

25 Q. You've said Active Directory a few times. What is Active

K25Wsch2

Weber - Direct

1 Directory?

2 A. Active Directory is a Microsoft product. Its job is user
3 authentication and permissions.

4 Q. Once a user had a DevLAN account, how would they log in to
5 DevLAN?

6 A. So, Typically, it would be with your Active Directory
7 credentials.

8 MR. LAROCHE: Ms. Hurst, you can pull down exhibit
9 1251. Thanks.

10 Q. Were there DevLAN computers in any other CIA facilities?

11 A. Yes, there were.

12 Q. Were those facilities located overseas in foreign
13 countries?

14 A. Yes, they were.

15 Q. How many overseas CIA facilities had access to DevLAN?

16 A. Two.

17 Q. I'm going to refer to them as Foreign Office East and
18 Foreign Office West. OK?

19 A. OK.

20 Q. How were the computers in those offices connected to the
21 DevLAN network?

22 A. They were routed over an agency network to access -- access
23 the portions of DevLAN, and while routed over the agency
24 portion of the network, we used what was referred to as
25 end-to-end encryption so that any traffic over the portion of

K25Wsch2

Weber - Direct

1 the network that we didn't control nobody else would be able to
2 access.

3 Q. What do you mean by agency network?

4 A. So, EDG is a very small portion of the agency. We owned
5 and maintained DevLAN, which was our network. The agency has
6 other portion -- or other networks for other purposes that are
7 run by, you know, somewhere -- other people in the agency.

8 Q. Is that the internet?

9 A. No, it's not.

10 Q. I think you also said end-to-end encryption. Is that
11 right?

12 A. Yes, I did.

13 Q. What is that?

14 A. End-to-end encryption is an industry term for when you --
15 when you are departing your one end point, so leaving your
16 segment of a local area network, and traveling to another end
17 point, every -- all of the communication in between those two
18 points is fully encrypted.

19 Q. Are you familiar with the term "network connectivity"?

20 A. Yes, I am.

21 Q. What does that term mean?

22 A. Network connectivity is the status of a machine's access to
23 network resources.

24 Q. What was the network connectivity like between the DevLAN
25 network in the CCI office and the DevLAN network located in

K25Wsch2

Weber - Direct

1 Foreign Office East and Foreign Office West?

2 A. The network connectivity within CCI's office was extremely
3 good. It was a very fast network.

4 Our connection to the field sites was extremely slow and
5 caused a lot of problems for our developers overseas.

6 Q. What do you mean by extremely slow?

7 A. The transferring of files that were not necessarily that
8 large in size sometimes could take longer than a day, and
9 that -- that caused issues because the -- our foreign offices
10 had to shut everything down at the end of the day and store it.
11 So if your transfer didn't complete in time, you had to start
12 it the next day and try again.

13 Q. And how big a transfer would take about a day for the
14 foreign office?

15 A. I don't remember the specifics. I remember working with
16 Frank, where Frank was trying to transfer a file that was only
17 a few megabytes in size and it taking hours.

18 MR. LAROCHE: Ms. Hurst, can you please publish
19 Government Exhibit 1026. If we could go to the first email on
20 this chain. Please just zoom in on the to-from line.

21 Q. I'm showing you another email. Do you see it on the screen
22 there, Mr. Weber?

23 A. Yes, I do.

24 Q. Who sent this email?

25 A. I did.

K25Wsch2

Weber - Direct

1 Q. Who did you send it to?

2 A. Patrick.

3 Q. When did you send it?

4 A. This would have been January 27, 2016, 9:07 p.m.

5 Q. And the subject is Bitbucket. What is Bitbucket?

6 A. Bitbucket was an Atlassian product. We've been referring
7 to it as Stash up at this point. Atlassian changed its name.

8 MR. LAROCHE: Ms. Hurst, can you just zoom in on the
9 text and the classification of this email.

10 Q. Did you classify this email?

11 A. Yes, I did.

12 Q. What did you classify it as?

13 A. Unclassified.

14 Q. Why?

15 A. So, the contents of this email, where I'm talking about a
16 blog post that Atlassian put on the internet, there's nothing
17 damaging in this email.

18 MR. LAROCHE: Ms. Hurst, can you zoom out and then go
19 to the next email in the chain, the response. Just go up one
20 more slide. I think at the bottom of this slide, if you can
21 zoom in on the "from."

22 Q. Did Patrick respond to you?

23 A. Yes, he did.

24 Q. And is this the response here?

25 A. Yes, it is.

K25Wsch2

Weber - Direct

1 Q. And when did he send the response?

2 A. January 28 at 4:57 a.m.

3 Q. Who did he send that to?

4 A. Myself and Josh Schulte.

5 MR. LAROCHE: We can zoom out. Go to the next page
6 and zoom in, at the top, including the classification. Sorry.
7 Just zoom out again, Ms. Hurst. I'm sorry. Just from the top
8 down through the classification. Thank you.

9 Q. And at the top here, is this additional people that Patrick
10 copied? Is that right?

11 A. Yes, it is.

12 Q. One of them is Frank. I think you referred to a Frank
13 earlier?

14 A. Yes, I did.

15 Q. Is it the same Frank?

16 A. Yes, it is.

17 Q. Who is Frank?

18 A. Frank was a developer in OSB that I worked closely with.
19 He eventually was selected for an overseas position.

20 Q. Did the classification level on the response by Patrick
21 change?

22 A. Yes, it did.

23 Q. How did it change?

24 A. It was up to secret.

25 Q. Is it possible to reclassify emails when you respond to

K25Wsch2

Weber - Direct

1 them?

2 A. Yes, it is.

3 Q. In what circumstances would that happen?

4 A. So, the scenario that you would up the classification of an
5 email is when your response contained classification -- or
6 classified information that was higher than the original
7 sending of that email.

8 Q. And this has a cross-through through the classification, is
9 that right?

10 A. Yes, it does.

11 Q. When you received this email communication, did it have
12 that cross-through?

13 A. No, it did not.

14 MR. LAROCHE: Ms. Hurst, can you zoom out, please, and
15 zoom in on the paragraph starting "additionally."

16 Q. Just read the first sentence, please, Mr. Weber.

17 A. "Additionally, could also get them to do some maintenance
18 on the DevLAN field connectivity."

19 Q. Do you understand what he's referring to there?

20 A. Yes.

21 Q. What was he referring to?

22 A. This -- there was both the speed of the connection as well
23 as they were not able to access all of the resources on DevLAN
24 that they were supposed to be able to access.

25 Q. Where was Patrick working at the time he sent this email?

K25Wsch2

Weber - Direct

1 A. He was in Foreign Office West.

2 MR. LAROCHE: Ms. Hurst, we can pull that email down.

3 Q. Now, you talked a little bit before about administrators of
4 the DevLAN network, is that correct?

5 A. That's correct.

6 Q. And you were also a user of that network?

7 A. That's correct.

8 Q. Generally speaking, what's the difference between a user
9 and an administrator?

10 A. The administrators provide access to the services. The
11 users are the ones that leverage the services for day-to-day
12 activities.

13 Q. Generally, do administrators have broader access to the
14 system?

15 A. Yes, they do.

16 Q. In what way?

17 A. They -- being administrators is a privileged position. You
18 have the keys to the kingdom for the services that you control.
19 You're able to modify who has access to what. You're able to
20 turn the service on, turn it off, all sorts of things like
21 that.

22 Q. Were there different types of DevLAN administrators?

23 A. Yes, there were.

24 Q. What were some of those types?

25 A. The DevLAN administrators kind of fell into three

K25Wsch2

Weber - Direct

1 categories. There were your true DevLAN administrators, who
2 were in ISB. Their job was specifically focused on the
3 administration of DevLAN, most specifically, Active Directory
4 and the network connectivity.

5 There were the Atlassian administrators, who were focused
6 solely on the Atlassian set of products. And then you would
7 have administrators for some of the software development
8 resources.

9 Q. What do you mean by that, that last piece?

10 A. So, a specific example was the OSB ESXi server was meant to
11 be a tool by developers for developers for development
12 activities, so there were some people that could maintain the
13 ESXi server.

14 Q. Let's start with the first group you mentioned, I think,
15 network-wide administrators, correct?

16 A. Yes.

17 Q. Who were the network-wide administrators as of 2015?

18 A. ISB.

19 MR. LAROCHE: Ms. Hurst, could you please publish to
20 the parties, the Court and the witness Government Exhibit 90.

21 Q. Do you recognize this?

22 A. Yes, I do.

23 Q. What is this?

24 A. This is another portion of the org structure of EDG.

25 Q. Does this fairly and accurately represent that portion of

K25Wsch2

Weber - Direct

1 the org structure of EDG?

2 A. Yes, it does.

3 MR. LAROCHE: Your Honor, we'd offer Government
4 Exhibit 90 in evidence.

5 MS. SHROFF: No objection, your Honor.

6 THE COURT: 90 is in evidence.

7 MR. LAROCHE: Thank you.

8 (Government Exhibit 90 received in evidence)

9 MR. LAROCHE: Please publish that to the jury, Ms.
10 Hurst.

11 Q. You've mentioned ISB a few times. Where was ISB within the
12 organizational structure of the group?

13 A. They were within SED.

14 Q. What was their role?

15 A. Their role was system administration.

16 Q. Did they have any development role?

17 A. No, they did not.

18 MR. LAROCHE: OK. We can pull that down, please.

19 Q. I think the second group of administrators you identified
20 on DevLAN were those who were in charge of the Atlassian
21 services. Is that correct?

22 A. That's correct.

23 Q. Was ISB in charge of the Atlassian services in 2015?

24 A. No, they weren't.

25 Q. Who were in charge of the Atlassian services as

K25Wsch2

Weber - Direct

1 administrators in 2015?

2 A. Originally, I believe it was Patrick. I think in early
3 2015 he had still an administrative role. Eventually that
4 transitioned to me, and I very quickly brought Josh on as an
5 administrator.

6 Q. As an administrator of the Atlassian services, what types
7 of things could you do?

8 A. The -- our roles and responsibilities were to keep the
9 service up and running, to ensure the backups of the service,
10 to provide user access to different portions of it, upgrade the
11 system, things like that.

12 Q. Now, you also said, I think, the third group was certain
13 hardware that there were administrators of. Is that correct?

14 A. Yes.

15 Q. And the example you gave was the ESXi server, is that
16 correct?

17 A. That is correct.

18 MR. LAROCHE: Ms. Hurst, can you please publish again
19 Government Exhibit 1290 and then just zoom in on ESXi server on
20 the top left.

21 Q. As of 2015 who were the administrators of the ESXi server?

22 A. I believe it was myself and Josh, for sure. I think Frank
23 was also an administrator, and Matt was also an administrator.

24 Q. And were all the individuals you just mentioned working
25 within OSB?

K25Wsch2

Weber - Direct

1 A. That is correct.

2 Q. As an ESXi administrator, what types of things could you
3 do?

4 A. As an ESXi administrator, your job was to be able to create
5 new virtual machines, power them on, power them off, back them
6 up, revert them to snapshots, things like that.

7 Q. You used the term "snapshot"?

8 A. That's correct.

9 Q. What does snapshot mean?

10 A. Snapshot is a term used with virtual machines. It is
11 creating -- creating a backup for the running state of a
12 machine at a given time. It's -- it's a tool that you can use
13 to back up your data.

14 Q. Did you ever crate snapshots of virtual machines?

15 A. Yes, I did.

16 Q. Why?

17 A. The most traditional-use scenario was if we were going to
18 upgrade the machine, you would create a backup right before
19 upgrading. That way, if there was a problem during the
20 upgrade, you could just revert to the snapshot and it was as if
21 it never happened.

22 Q. You also used the term "revert"?

23 A. Yes.

24 Q. What does that mean?

25 A. Revert is a term for saying discarding the current

K25Wsch2

Weber - Direct

1 machine's running state and returning it to a snapshot.

2 Q. In 2015, did ISB have a role as the ESXi server
3 administrator or Atlassian administrator?

4 A. I'm sorry. What was the date again?

5 Q. As of 2015.

6 A. As of 2015, they were not -- ISB was not the administrator
7 of the ESXi server.

8 Q. And what about the Atlassian services?

9 A. No, they were not.

10 Q. Why were they not acting in that administrative role?

11 A. ISB did not have the capacity. They didn't have enough
12 people to handle all of their responsibilities. Nor did they
13 have somebody that was qualified to handle the Atlassian
14 services.

15 Q. Let's talk for a moment about how you would log in as
16 administrator to the system.

17 A. OK.

18 Q. I first want to focus on the Atlassian-level administrator.

19 A. OK.

20 Q. How would you log in as an Atlassian-level administrator?

21 A. When you were interacting with the Atlassian service, that
22 was typically through the Atlassian -- like the web pages that
23 Atlassian presented, so you would navigate to
24 confluence.devlan.net, and you would be presented with a log-in
25 screen. You would give your Active Directory username and

K25Wsch2

Weber - Direct

1 credential to gain access to the system, and then if you were
2 going to do administrative activities, you would click on a
3 portion of the web page and get prompted for a username and
4 password again to validate that you were still the same
5 individual.

6 Q. Are you familiar with the term "SSH keys"?

7 A. Yes.

8 Q. What are those?

9 A. SSH keys are -- it is an alternative means of
10 authentication beyond a username and password that is more
11 secure.

12 Q. Why is it more secure?

13 A. So, most humans have a password that is going to be, you
14 know, between six and 12 characters, most likely. It's not --
15 it's not something that has that much random information in it.

16 An SSH key usually is around 4,096 bytes, so the amount of
17 random information in that key allowed for a much more secure
18 authentication.

19 Q. Were SSH keys used to log in as an Atlassian-level
20 administrator?

21 A. Through the website, no. But to access the servers that
22 they were running on, yes.

23 Q. And would that give you a different type of access?

24 A. Yes, it would.

25 Q. In what way?

K25Wsch2

Weber - Direct

1 A. So, the -- having access to the computer would allow us to
2 start and stop the Atlassian service. It would allow us to
3 upgrade it as well as access the file system, things like the
4 backups, stuff like that.

5 Q. And I know you said access to the server. Is that right?

6 A. Yes.

7 Q. In this context, are you referring to a virtual server?

8 A. I'm -- both, depending on the product. For Confluence and
9 Bamboo, I'd be referring to a virtual server. For Stash and
10 Jira, I'd be referring to a physical machine.

11 Q. Let's just talk about that for a moment. Looking at this
12 diagram, Confluence and Bamboo are running on virtual machines,
13 is that correct?

14 A. That's correct.

15 Q. Is that the same thing as a virtual server?

16 A. Yes.

17 Q. Why is that?

18 A. "Virtual server" is not an official term, so a server is
19 just a very powerful machine that has a specific purpose in
20 life.

21 Q. So you talked about logging in through the web with a
22 username and password as administrators, is that right?

23 A. Yes.

24 Q. And you talked about logging in to the virtual server using
25 SSH keys?

K25Wsch2

Weber - Direct

1 A. Yes.

2 Q. Now, there's also on this page an ESXi server, is that
3 correct?

4 A. That is correct.

5 Q. Were those different administrative privileges?

6 A. Yes, they were.

7 Q. How would you log in as an ESXi administrator?

8 A. There were multiple ways. The typical way was using a
9 product called vCenter or vSphere to log in via what was
10 effectively a web interface.

11 Q. How would you log in that way?

12 A. You would use your Active Directory credentials there as
13 well.

14 Q. And was there a specific route or administrative password
15 used to log in?

16 A. There was a backup route password that could be used.

17 Q. Was there another way to log into the server as an
18 administrator?

19 A. You could SSH into the server as well as physically access
20 the server as well; plug a keyboard into it and type a username
21 and password.

22 MR. LAROCHE: Ms. Hurst, could you please --

23 THE COURT: Mr. Laroche, would this be a convenient
24 time to take our morning break?

25 MR. LAROCHE: Yes, your Honor.

K25Wsch2

Weber - Direct

1 THE COURT: We'll take a 15-minute break.

2 (Jury not present)

3 THE COURT: See you in 15 minutes.

4 (Recess)

5 THE COURT: Please be seated.

6 (Jury present)

7 THE COURT: Please be seated.

8 Mr. Laroche.

9 MR. LAROCHE: Thank you, your Honor.

10 Q. Mr. Weber, we were talking before the break about logging
11 in as an administrator?

12 A. Yes.

13 Q. And one of the things we were talking about was logging in
14 to the OSB ESXi server.

15 A. Yes.

16 Q. I think you referred at one point to the word
17 "credentials"?

18 A. That's correct.

19 Q. What were you referring to there?

20 A. The credentials would be a username-and-password
21 combination. Typically, I'm referring to Active Directory
22 credentials.

23 Q. Just focusing on that server for a moment, the OSB ESXi
24 server --

25 A. Yes.

K25Wsch2

Weber - Direct

1 Q. -- how would you log in as administrator to that server?

2 A. Logging in to the OSB ESXi server, you would typically go
3 through vSphere to log in and do most of the administrative
4 functions, and you would log in using your Active Directory
5 credentials.

6 Q. You said vSphere?

7 A. Yes.

8 Q. What's vSphere?

9 A. It was -- it's a portion -- it's a product within the ESXi
10 tool suite that was meant to interface with an ESXi server.

11 Q. You also said earlier that you could log in using SSH keys,
12 is that correct?

13 A. That's correct.

14 Q. How would you do that?

15 A. You would use a -- any service that ran SSH, either a Linux
16 machine, or Windows had a tool like PuTTY installed on it, you
17 would leverage that to create an SSH access.

18 Q. What's PuTTY?

19 A. PuTTY's just a tool on windows that does communication like
20 SSH.

21 Q. And if you logged in using the SSH keys to the server, is
22 that different than logging in using the password?

23 A. It's -- the SSH key was set up for root, so you would be
24 logging in as the root user versus your admin credentials.

25 Q. What is the root user?

K25Wsch2

Weber - Direct

1 A. The root user, in this situation, "root" was kind of Linux
2 term for the administrative account on the machine, like the
3 default administrator account.

4 Q. You also mentioned there was a password for the ESXi
5 server?

6 A. That's correct.

7 Q. Was that password stored anywhere?

8 A. Yes, it was.

9 Q. Where?

10 A. It was stored on OSB's passwords page for some of our
11 services.

12 Q. What do you mean by OSB's passwords page?

13 A. OSB had a lot of virtual machines outside of the Atlassian
14 products that had passwords on them solely because the
15 technology required to have a password and not for security
16 practices, so that -- these were often like test machines, and
17 these passwords we kept on a page so that if somebody was
18 leveraging that VM they would have the credentials they needed
19 to log in to it.

20 Q. Where was that passwords page located?

21 A. Confluence.

22 Q. Was it restricted in any way?

23 A. It was.

24 Q. How?

25 A. It was to OSB.

K25Wsch2

Weber - Direct

1 MR. LAROCHE: Ms. Hurst, can you please publish
2 Government Exhibit 1003, and please just zoom in on the top of
3 the email, the to-from.

4 Q. Is this another email from the CIA, Mr. Weber?

5 A. Yes, it is.

6 Q. When was this email sent?

7 A. It was sent on March 31, 2015, at 8:20 p.m.

8 Q. Who sent it?

9 A. It was sent by Josh Schulte.

10 Q. Who was it sent to?

11 A. It was sent to the OSB email group.

12 Q. How do you know that?

13 A. The string NCS-IOC-EDG-AED-OSB is a user group and it's
14 explicit in its naming. NCS was in the org chart above IOC,
15 the rest of those are the groups that we have previously talked
16 about.

17 Q. It's a lot of acronyms.

18 A. It is.

19 Q. Below that, what's the subject line?

20 A. OSB.DevLAN.net VM credentials.

21 Q. What's OSB.DevLAN.net?

22 A. That was the OSB ESXi server.

23 MR. LAROCHE: Ms. Hurst, if you could please zoom out
24 and then on to the text of the email.

25 Q. Can you read the first sentence, please?

K25Wsch2

Weber - Direct

1 A. "I've modified the OSB's ESXi server page to contain the
2 passwords and other information directly instead of through the
3 OSB's passwords page; also updated the permissions to be
4 restricted to everyone outside of OSB."

5 Q. Do you understand what he's referring to by OSB's ESXi
6 server page?

7 A. Yes.

8 Q. What's he referring to?

9 A. It was a second page created later to contain information
10 specifically to the ESXi server and the administration of that.

11 Q. And do you understand what he means by updated the
12 permissions to be restricted to everyone outside of OSB?

13 A. This was him saying that only people within the OSB --
14 within OSB would have access to read this page.

15 Q. Now, is this the same ESXi server that as of 2015 was
16 running Confluence and Bamboo?

17 A. Yes, it was.

18 MR. LAROCHE: We can take that down. Thank you,
19 Ms. Hurst.

20 Q. Now, you've been testifying for quite a while now about
21 DevLAN, is that correct?

22 A. Yes.

23 Q. About its infrastructure and hardware and accesses, is that
24 right?

25 A. Yes.

K25Wsch2

Weber - Direct

1 MR. LAROCHE: Ms. Hurst, can you please publish
2 Government Exhibit 1251.

3 Q. Other than testifying today, have you ever spoken publicly
4 about DevLAN?

5 A. No, I have not.

6 Q. Why not?

7 A. The DevLAN -- the setup of DevLAN was classified, and
8 testimony about it or any discussion about it would give an
9 adversary, if they overheard that discussion, an adversary
10 insight into how the network was set up, what type of
11 technology it was running, things like that. This would create
12 a risk for the system because that's the first information you
13 need to effectively attack a target system.

14 Q. One of the parts of DevLAN you talked about was Hickok. Do
15 you recall that?

16 A. Yes.

17 Q. Other than testifying today, have you ever spoken publicly
18 about Hickok?

19 A. No.

20 Q. Why not?

21 A. The same reason.

22 Q. Is the DevLAN network still being used today?

23 A. No, it is not.

24 Q. When did DevLAN stop being used?

25 A. March 7.

K25Wsch2

Weber - Direct

1 Q. Of what year?

2 A. 2017.

3 Q. Why did it stop being used?

4 A. The disclosure of the WikiLeaks led to DevLAN essentially
5 being seen as a crime scene. We all stopped touching our
6 computers. The FBI came in and began confiscating all of the
7 equipment, and DevLAN ceased to exist.

8 Q. After the CIA stopped using the DevLAN network, did you
9 talk about it publicly?

10 A. No, I did not.

11 Q. Why not?

12 A. The -- even though DevLAN was eventually replaced by
13 another network, talking about DevLAN would still give an
14 adversary insight into the capabilities that the system
15 administration team had, and assuming you had the same system
16 admin team in place, an adversary would have the knowledge that
17 they would use the same technologies that they've used in the
18 past, because that's what they know.

19 Q. You've used the word "adversary" several times?

20 A. Yes.

21 Q. Who are you referring to?

22 A. I would most likely be referring to foreign entities that
23 are similar to CCI who are targeting the U.S. government.

24 MR. LAROCHE: You can take that down, please. Thank
25 you, Ms. Hurst.

K25Wsch2

Weber - Direct

1 Q. You testified earlier that the defendant became an
2 administrator Atlassian server, is that right?

3 A. Yes.

4 Q. When did that happen?

5 A. I believe it was summer of 2015.

6 Q. And you talked earlier about the various types of DevLAN
7 administrators?

8 A. Yes.

9 Q. What type of administrator did he become?

10 A. An Atlassian administrator.

11 Q. Did he also have a role with the ESXi server?

12 A. He did.

13 Q. What was that role?

14 A. He was an administrator of that. That would have been
15 before the summer of 2015, though.

16 Q. I want to focus you on the Atlassian administrative
17 privileges that he had.

18 A. Yes.

19 Q. How did it come about that he became an administrator?

20 A. Andrew -- I'm sorry. Patrick asked me to become an
21 administrator of the Atlassian products, and I -- I knew a
22 portion of what was needed for that. However, I was not a
23 Linux administrator by background, so I asked Josh to assist me
24 with this.

25 Q. What's Linux?

K25Wsch2

Weber - Direct

1 A. Linux is an operating system. Specifically, it was the
2 operating system that was running the Atlassian services.

3 Q. What's an operating system?

4 A. An operating system is -- that is the software that is used
5 for most of your operations. So, most people would recognize
6 windows. Windows is an operating system. Linux is another --
7 a competitor.

8 Q. Did the defendant have familiarity with that operating
9 system, Linux?

10 A. Yes, he did.

11 Q. At the point you asked him to help you with the
12 administration of the Atlassian services, approximately how
13 long had you worked with him?

14 A. That would have been about four, four or five years at that
15 point.

16 Q. At that point what was your relationship like?

17 A. I was close to him. I considered him a friend. We worked
18 closely on numerous products -- projects together. I trusted
19 him. I specifically reached out to him for this.

20 Q. What was the defendant's role as an Atlassian
21 administrator?

22 A. So, his main focus was on the Linux pieces of it, which
23 typically meant keeping the system up to date, start -- like
24 updating the Atlassian products. He set up the backups for us,
25 things like that. But generally, he -- he covered everything

K25Wsch2

Weber - Direct

1 when there was a time or a need.

2 Q. Who defined his role as an administrator?

3 A. I did.

4 MR. LAROCHE: Ms. Hurst, can you please publish
5 Government Exhibit 1251 again.

6 Q. At the time the defendant became an Atlassian
7 administrator, were the Atlassian services being backed up to
8 the Altabackups?

9 A. No, they were not.

10 Q. Where were they being backed up at that point?

11 A. They were being backed up locally.

12 MR. LAROCHE: If we could just zoom in again on the
13 ESXi server.

14 Q. Just to focus on Confluence, what do you mean that the
15 backups were being backed up locally at that point?

16 A. Confluence had a hard drive assigned to it, and the same --
17 the same location. Different file path, but essentially the
18 same location the original data was being written to the backup
19 data was being written to.

20 MR. LAROCHE: Ms. Hurst, if we could zoom out again.
21 Thank you.

22 Q. Did the defendant have a role in changing where the backups
23 were stored?

24 A. Yes.

25 Q. What was his role?

K25Wsch2

Weber - Direct

1 A. After the Altabackup folder was created, Josh was the one
2 that modified the Linux machines to be able to access that
3 folder and modified the Atlassian scripts that executed the
4 backup to write to the new location.

5 Q. Let's start with the scripts.

6 A. OK.

7 Q. What is a script?

8 A. It's a series of commands that a computer would execute.

9 Q. Why did he need to modify the script?

10 A. The scripts were set up to write in one location, the local
11 location. It needed to be changed to the remote location.

12 Q. The other thing you said he did was modify the machines, is
13 that right?

14 A. That is correct.

15 Q. How did he modify the Linux machines?

16 A. The Linux machines needed to have access to the remote
17 storage location, so he ran a command called mount that would
18 allow, allow that network location to be accessed like any
19 other folder on the system.

20 Q. Are you familiar with the term "mount point"?

21 A. That's correct -- yes, I am.

22 Q. What's a mount point?

23 A. A mount point is essentially the -- like the information
24 needed to say, you know, this either hard drive, remote
25 location, whatever, is connected to this computer and this is

K25Wsch2

Weber - Direct

1 how you access it.

2 Q. Did the defendant help create mount points for the
3 Altabackups?

4 A. Yes.

5 Q. What did he do?

6 A. He ran the mount command, which is what's used to create a
7 mount point.

8 Q. What was the purpose of those mount points?

9 A. To ensure that the VMs had access to the NetApp location.

10 Q. You said VMs. What do you mean by that?

11 A. The Confluence VM, Bamboo VM or the Stash server or the
12 Jira server.

13 Q. Where were those mount points located?

14 A. The mount points were located within the operating system
15 on its file system.

16 Q. Did each Atlassian service have its own mount point?

17 A. Yes, that's correct.

18 Q. Why would they each need their own mount point?

19 A. They were each running on their own operating system.

20 Q. Could regular DevLAN users access those mount points?

21 A. No.

22 Q. Why not?

23 A. They didn't have access to them, and they didn't -- we
24 didn't publish the location of them.

25 Q. Could regular DevLAN users access the backups in any other

K25Wsch2

Weber - Direct

1 way?

2 A. No, I don't believe so.

3 Q. Could an Atlassian administrator access the Altabackups
4 using those mount points?

5 A. That is correct.

6 Q. How?

7 A. You -- if you log in to the virtual machine itself or the
8 physical machine and -- you'd be able to navigate to the mount
9 point just like you would navigate to any other folder on the
10 system.

11 Q. And once you went to the mount point, where would that take
12 you?

13 A. The NetApp storage location.

14 Q. For the Altabackups?

15 A. Correct.

16 Q. After the defendant helped set up the mount points for the
17 Altabackups, did you tell the other developers about the
18 Altabackups?

19 A. No, I did not.

20 Q. Why not?

21 A. There was no reason to publish that information. The other
22 developers wouldn't care.

23 MR. LAROCHE: Ms. Hurst, we can put pull that down.

24 Thank you.

25 Q. Now, you said in 2015 the infrastructure support, ISB was

K25Wsch2

Weber - Direct

1 not acting as the administrator of the Atlassian services, is
2 that right?

3 A. Yes, that is correct.

4 Q. Did you have discussions with the defendant about that?

5 A. Yes.

6 Q. When, approximately, did those discussions occur?

7 A. I would -- it's safe to say that it was pretty much the
8 extent, every single day that we were doing administrative
9 activities via Atlassian.

10 Q. Could you describe those discussions?

11 A. The Atlassian administration duties were an additional duty
12 as assigned. It was not our day-to-day job, and it distracted
13 us from our day-to-day job, so it was, you know, not something
14 that we looked forward to doing and did not want to be doing
15 it.

16 Q. Did the defendant complain about the fact that ISB was not
17 acting as the Atlassian administrator?

18 A. Yes.

19 Q. What types of things would he say?

20 A. It would be along the lines of, you know, we would be
21 complaining about the fact that we would have deadlines on
22 other projects but we're focused on fixing something in the
23 Atlassian product or doing something. It was an significant
24 amount of additional work, so the complaints were along those
25 lines.

K25Wsch2

Weber - Direct

1 Q. Other than the defendant's complaints about ISB's roles,
2 did the defendant make any other complaints about the Atlassian
3 services on DevLAN?

4 A. No.

5 Q. Did the defendant ever complain that the Atlassian services
6 were vulnerable to theft?

7 A. No.

8 Q. Are you sure about that?

9 MS. SHROFF: Objection, your Honor.

10 THE COURT: Overruled.

11 MS. SHROFF: It's hearsay.

12 THE COURT: Overruled.

13 BY MR. LAROCHE:

14 Q. Are you sure that the defendant never made any complaints
15 that DevLAN was vulnerable to theft?

16 A. Yes.

17 Q. Why?

18 MS. SHROFF: Objection.

19 THE COURT: Overruled.

20 A. If he had complained to me about the Atlassian products
21 being vulnerable to theft, I would have told him to fix it.
22 The Atlassian products were our responsibility, and if he had
23 highlighted an issue with that, I would have made it our
24 primary focus to fix that.

25 MR. LAROCHE: Ms. Hurst, can we please publish

K25Wsch2

Weber - Direct

1 Government Exhibit 1012, please. If we could just focus on the
2 bottom to-from line.

3 Q. Is this another email sent from the CIA, Mr. Weber?

4 A. Yes, it is.

5 Q. Who sent this email?

6 A. Josh.

7 Q. And when did he send it?

8 A. This would have been August 11, 2015, at 7:37 p.m.

9 Q. Who did he send it to?

10 A. This would have been sent to the email group for AED, and
11 he also copied the email group for ISB.

12 Q. What's the subject line?

13 A. Complete Atlassian server outage.

14 Q. This was 2015, is that correct?

15 A. Yes.

16 Q. Was he acting as the Atlassian administrator at this time?

17 A. Yes, he was.

18 MR. LAROCHE: Could you zoom out to the text of the
19 email, please.

20 Q. Could you summarize what he's saying in this email?

21 A. Yes. So, at this time if a user tried to log in to any of
22 the Atlassian products, they would not have been able to, so
23 essentially the Atlassian products were down for use. This was
24 due to an issue connecting to the Active Directory server that
25 Crowd needed to be able to provide access to the products.

K25Wsch2

Weber - Direct

1 Q. Why did you need ISB's help to resolve this issue?

2 A. ISB was the ones who ran the Atlassian products -- sorry,
3 Active Directory. And this was an issue querying the Active
4 Directory platform.

5 MR. LAROCHE: Could we zoom out for a second,
6 Ms. Hurst.

7 Q. Was this problem resolved?

8 A. Yes, it was.

9 Q. How do you know that?

10 A. The next email, which I sent, says the log-in issue has
11 been resolved.

12 MR. LAROCHE: We can pull that down. Thank you.

13 Q. Were there discussions about transitioning Atlassian
14 administration to ISB?

15 A. From the day we brought it into -- into EDG.

16 Q. How often did you have those discussions?

17 A. Numerous. I would say monthly, most likely.

18 Q. Did that transition happen quickly?

19 A. No, it did not.

20 MR. LAROCHE: Let's look at Government Exhibit 1017.
21 Could we just focus on the top, to-from line.

22 Q. Is this another email from the CIA?

23 A. Yes.

24 Q. Who sent it?

25 A. I did.

K25Wsch2

Weber - Direct

1 Q. When did you send it?

2 A. This would have been October 2015, October 6, 2015.

3 Q. Who did you send it to?

4 A. José.

5 Q. Where did José work at the time?

6 A. He was in ISB.

7 Q. Did you copy anyone on this email?

8 A. Yes, I did.

9 Q. Who did you copy?

10 A. Robert, Sean and Josh.

11 Q. Who's Sean?

12 A. Sean was my branch chief.

13 Q. Which branch?

14 A. He was chief of OSB.

15 Q. And the subject is infrastructure running on OSB's server,
16 is that right?

17 A. Yes.

18 Q. Is this the ESXi server you referred to earlier?

19 A. Yes, it is.

20 MR. LAROCHE: If we could just zoom out for a second
21 and then zoom in on the first paragraph.

22 Q. Read the first sentence, please.

23 A. "Below is a list of what we have running on our server, all
24 of which we are looking to migrate to you guys when you have
25 the horsepower."

K25Wsch2

Weber - Direct

1 Q. What did you mean by that?

2 A. If I recall correctly, ISB was standing up some new ESXi
3 server infrastructure. Once they had that server
4 infrastructure in place, that's what I mean in terms of
5 horsepower.

6 Q. And can you read the second sentence, please?

7 A. "The list is in priority order, but the three in red should
8 be considered high priority since they contain data needed for
9 day-to-day operations (*i.e.*, the pitchforks come out when they
10 go down)."

11 MR. LAROCHE: Could we zoom out, Ms. Hurst, and could
12 we zoom in on the three in red. Thank you.

13 Q. Starting at the top, it says machine at the top left?

14 A. Yes.

15 Q. What's that referring to?

16 A. In this case it was the virtual machine running Confluence.

17 Q. And then below that there's another machine?

18 A. Yes.

19 Q. What's that?

20 A. Bamboo.

21 Q. Were these the virtual machines running on the ESXi server?

22 A. Yes, they were.

23 Q. When you talked about being an Atlassian administrator, did
24 you have Atlassian administrative services for these virtual
25 machines?

K25Wsch2

Weber - Direct

1 A. Administrative access to these machines?

2 Q. Yes.

3 A. Yes, that is correct.

4 MR. LAROCHE: We can zoom out.

5 We can pull this email down.

6 Q. After you sent this email, did ISB move Confluence and
7 Bamboo to their infrastructure?

8 A. Not immediately. It took a significant amount of time.

9 MR. LAROCHE: Let's look at Government Exhibit 1024
10 and just zoom in on the to-from at the top.

11 Q. When was this email sent?

12 A. January 14, 2016.

13 Q. Who sent it?

14 A. Josh Schulte.

15 Q. And who did he send it to?

16 A. This was sent to the AED group as well as the ISB group.

17 Q. And what was the subject of this email?

18 A. Atlassian support transition to ISB.

19 MR. LAROCHE: If we can zoom out for a second and then
20 zoom in on the text of the email.

21 Q. Could you read the first sentence, please?

22 A. "We are currently transitioning the Atlassian product
23 support from OSB to ISB (POC Rufus)."

24 Q. Who is Rufus?

25 A. Rufus was somebody hired by ISB to specifically manage the

K25Wsch2

Weber - Direct

1 Atlassian products.

2 Q. Did that transition happen in January of 2016?

3 A. No, it did not.

4 Q. Why not?

5 A. Rufus departed after a couple of weeks working with EDG.

6 MR. LAROCHE: You can pull that down.

7 Q. Now, in addition to helping to design and run the Atlassian
8 services, did the defendant also develop cyber tools?

9 A. Yes, that is correct.

10 Q. Generally speaking, what types of cyber tools did the
11 defendant work on?

12 A. Josh's main focus was on tools for operations when we had
13 physical access to a target machine.

14 Q. What do you mean by physical access?

15 A. Physical access would be when an agency officer or asset
16 was willing to touch a machine for us, maybe type on a
17 keyboard, maybe plug in a thumb drive into it, or walk off with
18 the machine.

19 Q. Did the defendant work with other developers on some of his
20 projects?

21 A. Yes.

22 Q. Do you know a developer named Amol?

23 A. Yes, I do.

24 Q. What branch within the group did Amol work in?

25 A. For the majority of his time with EDG, it was OSB.

K25Wsch2

Weber - Direct

1 Q. How often did you interact with Amol while he was with OSB?

2 A. Pretty much daily.

3 Q. Would you describe those interactions?

4 A. I would consider Amol a friend. We talked often. We -- we
5 collaborated together. At the time Amol was hired, I had a
6 project that a significant portion of my career had been spent
7 on but I was transitioning off of, and I selected Amol to take
8 over that project.

9 Q. Did Amol start working with the defendant on projects?

10 A. Yes, he did.

11 Q. Approximately when did he start doing that?

12 A. I believe it was almost immediately.

13 Q. Was there a specific project that he assisted the defendant
14 with?

15 A. Yes.

16 Q. What was that project called?

17 A. Brutal Kangaroo and Drifting Deadlines.

18 Q. Did you observe the defendant and Amol interact?

19 A. Yes.

20 Q. How often, roughly?

21 A. I sat next to Josh and Amol, so any time I was at my desk
22 and they were interacting, I would witness it.

23 Q. Could you describe those interactions.

24 A. They -- they ran the gamut. Sometimes they were completely
25 professional, back and forth on how to approach a problem, but

K25Wsch2

Weber - Direct

1 oftentimes, they were less than professional. And Josh and
2 Amol did not get along personally.

3 Q. Did those interactions change over time?

4 A. It was a continuous downhill relationship.

5 Q. What do you mean by downhill relationship?

6 A. So, Josh and Amol rubbed each other the wrong way. That
7 was obvious early on, and there was increasing animosity
8 between the two of them as long as they were working together.

9 Q. Did you attempt to intervene between them?

10 A. Numerous times.

11 Q. How did you attempt to do that?

12 A. I would often talk to either Amol or Josh after a
13 less-than-professional interaction and try and tell them to,
14 you know, knock it off or calm down.

15 Q. Now, you said one of the tools that they were working on
16 together was Drifting Deadlines, is that correct?

17 A. Yes.

18 Q. In early 2016, did an issue arise regarding Drifting
19 Deadlines?

20 A. Yes.

21 Q. What happened?

22 A. Drifting Deadlines was supposed to meet a specific
23 operational need. COG needed it as soon as possible. The tool
24 was aptly named because it was constantly missing delivery
25 milestones and deadlines, so COG requested that EDG create

K25Wsch2

Weber - Direct

1 another, similar capability through an external contractor.

2 Q. What do you mean by that?

3 A. We paid a external company to create a tool for us.

4 Q. Did you talk to the defendant about that?

5 A. Yes.

6 Q. What did he say?

7 A. Josh was offended by this, for multiple reasons. One, he
8 saw it as a, like he saw it as a lack of trust in him as a
9 developer, that he would not be able to deliver the capability
10 in time. But he also thought that the government was going to
11 be defrauded because his and Frank's hard work, he thought, was
12 going to be given to this contractor to be, in turn, sold back
13 to the U.S. government.

14 Q. Was that true?

15 A. No, it was not.

16 Q. How do you know that?

17 A. That's not the way the contract was set up. The contractor
18 was going to get capability that they would incorporate into
19 their tool, but that was not going to be charged to the U.S.
20 government. We have --

21 MS. SHROFF: Your Honor, we object to this testimony.

22 THE COURT: Overruled.

23 MS. SHROFF: It's not from something he personal his
24 knowledge.

25 THE COURT: Don't interrupt. It's overruled.

K25Wsch2

Weber - Direct

1 A. We also have people in the agency whose job is to manage
2 these interactions with contracts on a daily basis, and their
3 job is to make sure that everything is in the best interests of
4 the government.

5 Q. Did there come a time when there was a meeting about this
6 contractor issue?

7 A. Yes.

8 Q. When, approximately?

9 A. It was, I believe, in April of 2016, early 2016.

10 Q. Who participated in that meeting?

11 A. The meeting was intended to be between the contractor,
12 the -- my branch chief, Sean, Frank, as well as that government
13 POC that I referenced earlier.

14 Q. Did the defendant participate in this meeting?

15 A. Yes, he did.

16 Q. Was he invited to the meeting?

17 A. No, he was not.

18 Q. How do you know he was not invited to the meeting?

19 A. I was -- again, I sat next to Josh. I also sat next to
20 Frank. I was there when Sean came to get Frank to go to this
21 meeting. Josh requested to attend. He was told not to go, and
22 Josh said that he was going to go anyway.

23 Q. Did he say anything else to Sean at that time?

24 A. I remember it being along the lines of fuck you, I'm going
25 anyway.

K25Wsch2

Weber - Direct

1 Q. After the meeting, did you speak with the defendant?

2 A. Yes.

3 Q. Did you talk about this issue again?

4 A. Yes.

5 Q. What was his demeanor like during those interactions?

6 A. So, I had a conversation with him, talking about how -- I
7 was trying to get him to realize that the actions he took were
8 a slap in the face to Frank and Sean, somebody that I respected
9 greatly, and that he needed to trust in them, that this was
10 doing the right thing and that, furthermore, his actions
11 were -- you know -- he was burning bridges. He was making it
12 hard so that people would not want to work with him in the
13 future, things like that.

14 Q. Why did you say it was a slap in the face to Frank and
15 Sean?

16 A. So, Frank and Sean, numerous times, explained to Josh was
17 going on and that it was OK, and Josh was telling them that
18 they were wrong.

19 Q. How did he react to your conversations with him about this?

20 A. Sort of a lot of similar conversations like this with Josh,
21 he -- he would often acknowledge my viewpoint, and then we
22 would move on.

23 Q. Around this time, did you also talk to the defendant about
24 someone named Karen?

25 A. Yes.

K25Wsch2

Weber - Direct

1 Q. Who is Karen?

2 A. Karen was our group chief, chief of EDG.

3 MR. LAROCHE: If we could just publish Government
4 Exhibit 89 again.

5 Q. So where did Karen fall within this organizational chart?

6 A. She would have been in charge of EDG.

7 Q. How many levels of management were between you as a
8 developer and Karen as chief of EDG?

9 A. So, it would have went my branch chief, the division chief
10 and deputy division chief and then deputy group chief and then
11 Karen, the group chief.

12 Q. What types of things would the defendant say about Karen?

13 A. He --

14 MS. SHROFF: Objection as to hearsay.

15 THE COURT: Overruled.

16 A. He often was derogatory to her. He did not -- he did not
17 agree with the direction of her leadership AND would often
18 vocally state that.

19 Q. What do you mean by derogatory towards her?

20 A. Comments like dumb bitch would occasionally be thrown
21 around.

22 Q. Did you respond to him about that?

23 A. Yes.

24 Q. What did you say?

25 A. I -- again, I would counsel him often on his actions. I

K25Wsch2

Weber - Direct

1 respected Karen a great deal, and I thought she was one of the
2 better group chiefs we had had, so I was trying to get him to
3 understand the realities.

4 Q. How, if at all, did the defendant respond to that?

5 A. Very similar to other conversations I had with him. You
6 know, he would acknowledge my viewpoint, not necessarily change
7 his actions after the conversation.

8 MR. LAROCHE: Ms. Hurst, we can pull that exhibit
9 down. Thank you.

10 Q. We just talked for a minute about an issue with Drifting
11 Deadlines?

12 A. Yes.

13 Q. That occurred in early 2016, is that right?

14 A. Yes.

15 Q. Around the time of this issue, was the defendant still
16 working with Amol?

17 A. Yes, I believe so.

18 Q. Did you observe any changes in their relationship?

19 A. It -- it was extremely strained at this point in their
20 relationship.

21 Q. Did there come a time when you observed an argument between
22 them?

23 A. Yes.

24 Q. When, approximately, did that happen?

25 A. I believe it was if not immediately following the meeting

K25Wsch2

Weber - Direct

1 that we just talked about or the next day. Josh and Amol got
2 into an argument about Josh's actions during -- during that
3 meeting and the fact that he forced himself into that meeting,
4 and it got heated.

5 Q. Did you attempt to intervene in the dispute?

6 A. Yes.

7 Q. How did you attempt to intervene?

8 A. I told them both to stop it. Specifically, I told Josh to
9 be the bigger man and walk away from the argument.

10 Q. What, if anything, did he say in response to that?

11 A. Josh said, We all know who the bigger man is, in reference
12 to Amol's weight.

13 Q. What did you understand the defendant to mean by that?

14 A. He was calling Amol fat.

15 Q. What, if anything, did you do in response to this
16 interaction?

17 A. I had a very long discussion with Josh immediately after,
18 trying to get him to realize that he was doing everything in
19 his power to make sure any relationships he had within the
20 agency were burnt, and that this was going to make it hard for
21 people to work with him in the future and it's going to make
22 him hard to be promoted.

23 Q. How did he react to that conversation?

24 A. Same as always, like he was still a little bit heated, he
25 acknowledged my viewpoint, and we moved on.

K25Wsch2

Weber - Direct

1 Q. Did you tell anyone else about the interaction you observed
2 between Amol and the defendant?

3 A. The conversation we had was not in a private location, so
4 some people overheard it. We -- we talked about the
5 interaction in general as well the next day.

6 Q. Did there come a time when you talked to Sean, the branch
7 chief, about it?

8 A. Yes.

9 Q. When, approximately?

10 A. I believe it was the next day.

11 Q. And what happened?

12 A. I went into Sean's office, and I wanted to know if he
13 wanted me to take a more active role in trying to get Amol and
14 Josh to play well together. And at that point Sean told me
15 that it was beyond us now.

16 MS. SHROFF: Objection, your Honor. Continued
17 hearsay.

18 THE COURT: Overruled.

19 Q. After that conversation with Sean, did you learn that the
20 defendant had made a complaint against Amol?

21 A. Yes.

22 Q. How did you learn that?

23 A. I don't remember how I first learned it, if it was just
24 through talking to the other developers who had already
25 discovered it, if I was officially told about it from

K25Wsch2

Weber - Direct

1 management, or if I saw Josh's complaint.

2 (Continued on next page)

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

K253SCH3

Weber - Direct

1 Q. Did you ever review the defendant's complaint against Amol?

2 A. Yes, I did.

3 Q. Did the defendant try to show it to you?

4 A. He did, yes.

5 Q. Did the defendant try to show it to others in the branch?

6 A. Yes.

7 Q. What, if anything, did you see in terms of how others in
8 the branch reacted to that?

9 A. The other -- the other members of the branch were annoyed
10 by the situation.

11 Q. Why?

12 A. They --

13 MS. SHROFF: Objection.

14 THE COURT: Overruled.

15 A. They felt like they were getting --

16 MS. SHROFF: Objection.

17 THE COURT: Overruled.

18 A. They felt that they were being pulled into a personal issue
19 between Josh and Amol. Furthermore, Josh's complaint
20 specifically --

21 MS. SHROFF: Objection, your Honor.

22 THE COURT: Overruled, Ms. Shroff.

23 A. Josh's complaint specifically called out some of us as
24 being targets of Amol as well, which was false.

25 Q. Did there come a time when you actually saw that complaint?

K253SCH3

Weber - Direct

1 A. Yes.

2 MR. LAROCHE: Ms. Hurst, can you please publish
3 Government Exhibit 1038 and page four of that exhibit.

4 Q. Mr. Weber, do you recognize this?

5 A. Yes, I do.

6 Q. Do you recognize the handwriting?

7 A. Yes, I do.

8 Q. Whose handwriting is it?

9 A. Josh Schulte's.

10 Q. Is this the complaint you were referring to earlier?

11 A. Yes, it is.

12 Q. If we can go to the next page. Mr. Weber, have you seen
13 this next page?

14 A. Yes, I have.

15 Q. Is this, from your view, a typed up version of the
16 handwritten complaint?

17 A. Yes, it is.

18 Q. So let's focus on this one. It is a little easier to read.

19 A. Okay.

20 Q. If we can focus on the first paragraph, please.

21 A. Do you want me to read it?

22 MS. SHROFF: Your Honor, could the government clarify
23 who typed this up, and when it was typed and when it was
24 created?

25 THE COURT: Mr. Laroche?

K253SCH3

Weber - Direct

1 MR. LAROCHE: It is attached to the e-mail that's been
2 entered into evidence.

3 MS. SHROFF: That does not clarify the issue, your
4 Honor.

5 THE COURT: That's the best we can do.

6 Q. Please read the first sentence.

7 A. "Dating back to August of 2015, Amol has made very
8 derogatory and abusive comments to myself and my colleagues."

9 Q. You ever observe Amol make very derogatory or abusive
10 comments to his co-workers?

11 A. No.

12 Q. Did you ever observe the defendant make derogatory or
13 abusive comments to his co-workers?

14 A. Yes.

15 Q. Without discussing the substance of those comments, how
16 often did he do so?

17 A. It was not a regular occurrence. But, Josh, Josh's poking
18 of fun at other developers would occasionally cross a line.

19 Q. Please read the second sentence.

20 A. "These dark and disparaging comments include 'I wish you
21 were dead,' 'I want to piss on your grave,' 'I want to dance on
22 your grave,' 'I wish you'd die in a fiery crash and burn, oh I
23 would be so happy.' 'I only say I wish you'd die because I
24 really wish it were true.'"

25 Q. Did you ever observe Amol make these kind of comments?

K253SCH3

Weber - Direct

1 A. Similar comments.

2 Q. Can you give some context to how these comments were made?

3 A. They --

4 MS. SHROFF: Objection.

5 THE COURT: Overruled.

6 A. It was usually after Josh had been having a long
7 conversation with Amol about anything from the way a project
8 could go, or things like that. It would usually be, like I
9 said earlier, when Josh -- when Josh had set a path on
10 something, it was hard to sway him. And the conversations
11 could go for an extensive time, it would often exhaust you.
12 So, Amol, after being in one of these conversations with Josh,
13 would often, like, sigh, lean up against a wall, and just say
14 something like this.

15 Q. Did the defendant ever tell you he was fearful of Amol
16 based on those comments?

17 A. No, he did not.

18 Q. Did you ever talk to Amol about those comments?

19 A. No.

20 Q. Why not?

21 A. It's -- Josh never expressed a concern over it. Often Josh
22 would actually laugh following comments like this. So, it was,
23 just never felt a need to bring it up.

24 Q. If we can go to the second paragraph, please. Can you read
25 this paragraph, please.

K253SCH3

Weber - Direct

1 A. "Specifically, on Monday, February 29, 2016, during the
2 midmorning, I walked into work to Amol berating me with
3 comments such as 'bald asshole,' insulting my work, and stating
4 that I will never get promoted past a 12 due to my poor work
5 quality and work ethic. I responded stating that at least I
6 can program. This infuriated Amol because usually people do
7 not respond to his bullying or attempt to fight back."

8 Q. Did you observe this interaction?

9 A. No, I did not.

10 Q. The last sentence says "usually people do not respond to
11 his bullying or attempt to fight back."

12 Did you ever observe Amol bully anyone?

13 A. No, I did not.

14 Q. If we can go to the third paragraph, please. Can you
15 please read that.

16 A. "For the remainder of Monday and into Tuesday, Amol was
17 very visibly distraught and upset. His behavior was out of the
18 ordinary, and he was unusually quiet. On Tuesday, March 1st,
19 2016, during the midmorning, I noticed Amol about to leave his
20 work station. I turned, facing away from him, and inquired
21 about a project we were working on. The next thing I knew,
22 Amol was directly behind me, unusually close, towering over me.
23 I was caught offguard and afraid. He then, through gritted
24 teeth, angrily said, 'I wish you were dead, and that's not a
25 threat, it's a fucking promise.' I was afraid that he might

K253SCH3

Weber - Direct

1 stab me or assault me in some way. I was frightened and very
2 concerned especially based on his behavior. I thought he may
3 harm myself or others, so I contacted security at the end of
4 the day to report these events."

5 Q. Did you ever see Amol do any these things?

6 A. No.

7 Q. We can pull that down.

8 After the defendant made these allegations against
9 Amol, did you talk to the defendant about them?

10 A. No, I did not.

11 Q. Why not?

12 A. After seeing these allegations, I felt that Josh was lying,
13 which I felt crossed a line, and I just was done with him. I
14 didn't consider him a friend anymore. And I didn't want to
15 deal with him or the drama around him.

16 Q. Why did you think he was lying?

17 A. I work closely with Amol. I didn't believe the comments, I
18 had never seen an interaction like that, and the interactions
19 that I did reference, or did see, I felt like Josh took
20 significantly out of context to try and support his viewpoint.

21 Q. After the defendant made these allegations, were Amol and
22 the defendant physically separated within the branch?

23 A. Yes, they were.

24 Q. How were they separated?

25 A. Amol was asked to move desks, and then shortly after, Josh

K253SCH3

Weber - Direct

1 was asked to change desks as well.

2 MR. LAROCHE: Ms. Hurst, can you please publish
3 Government Exhibit 111. If we can just zoom in on the lower
4 left of the screen maybe to about the middle. It's over just a
5 little bit to the right as well.

6 Q. Do you see OSB on Government Exhibit 111?

7 A. Yes, I do.

8 Q. Just remind us, before they were moved, where were you
9 sitting in OSB?

10 A. Wait, I'm sorry. I believe this is the eighth floor.

11 MR. LAROCHE: We need the next page. Sorry.

12 Q. Do you see OSB on this page?

13 A. Yes, I do.

14 Q. This is the ninth floor, for orientation?

15 A. Yes, it is.

16 Q. Can you just circle where you sat in OSB as of 2015 and
17 2016.

18 And before the move happened, please circle first
19 where Josh sat. And that's next to you; is that correct?

20 A. That is correct.

21 Q. Then where did Amol sit? Okay.

22 Can you now circle or just mark with an X first where
23 Josh was moved to within branch.

24 And then with another X, where was Amol moved to
25 within branch.

K253SCH3

Weber - Direct

1 How did the defendant react to having to move desks?

2 A. He was offended.

3 Q. Why do you say that?

4 A. He stated that this was a retaliation against him, and it
5 was unfair.

6 Q. Did he actually move desks?

7 A. No.

8 Q. Why do you say that?

9 A. He, he would move a couple personal items, and then return
10 to his desk, to do his day-to-day work, until -- until Sean
11 came and asked him again to move. And he would repeat the
12 process. He never completed the move.

13 MR. LAROCHE: We can pull that down, please, thank
14 you.

15 Q. The complaint that we just reviewed, was that an internal
16 complaint to the CIA?

17 A. Yes, it was.

18 Q. Other than making that internal complaint to the CIA, did
19 the defendant make any other complaints outside the CIA against
20 Amol?

21 A. Yes.

22 Q. What did he do?

23 A. He filed a restraining order.

24 Q. When approximately did he do that?

25 A. I believe it was shortly after the incident.

K253SCH3

Weber - Direct

1 Q. Where did he file that restraining order?

2 A. In Loudoun County.

3 Q. After the defendant filed that restraining order, did he
4 and Amol remain in OSB?

5 A. No.

6 Q. What happened?

7 A. Amol was moved to MSB, and Josh was moved to RDB.

8 Q. What does RDB stand for?

9 A. Remote Development Branch.

10 Q. If we can pull up Government Exhibit 89. You see RDB on
11 this organizational chart?

12 A. Yes, I do.

13 Q. Generally speaking, what type of work does RDB do?

14 A. RDB was focused on remote operations. These would have
15 been scenarios where we had somebody communicating with a -- a
16 target machine over the internet.

17 Q. Is moving to RDB from OSB a demotion?

18 A. No, it's not.

19 Q. Why not?

20 A. It's a sister branch. It's, it's a different focus for
21 type of work, but it was -- it was not a junior branch in any
22 way.

23 Q. How did the defendant react to being moved to RDB?

24 A. He -- I don't actually know. I wasn't interacting too much
25 with him about -- I don't know how he reacted to going to RDB

K253SCH3

Weber - Direct

1 specifically.

2 Q. At the time, where was RDB located?

3 A. They were on the eighth floor.

4 Q. We can pull that down, please.

5 So other than reporting the incident to internal
6 security and filing a protective order, did the defendant take
7 any other action against Amol?

8 A. Yes.

9 Q. What did he do?

10 A. He filed an EEO complaint.

11 Q. What is EEO?

12 A. Equal employment opportunity.

13 Q. How did you learn that the defendant filed an EEO
14 complaint?

15 A. I, I don't remember specifically how I was first told about
16 it. But, eventually, I was asked to make an official statement
17 regarding it.

18 Q. Why were you asked to make an official statement?

19 A. He referenced me in the EEO complaint.

20 Q. Were you asked to respond to any specific allegations?

21 A. All of the allegations.

22 Q. What do you remember responding to?

23 A. So, the specific ones that I remember responding to were,
24 one, that Amol would often call my wife dumb, and secondly that
25 Amol would make racist comments frequently.

K253SCH3

Weber - Direct

1 Q. Were either of those things true?

2 A. No.

3 Q. You said that the defendant moved to RDB after filing the
4 protective order; is that right?

5 A. Yes.

6 Q. When the defendant moved to a different branch, did he
7 continue working on his old branch projects?

8 A. Not initially.

9 Q. Why not?

10 A. He was in a different branch now. He was supposed to focus
11 on that branch's work.

12 Q. Did the defendant lose privileges on DevLAN to his old
13 branch's projects?

14 A. Yes.

15 Q. What, if anything, was done to do that?

16 A. He was removed. If he was a project lead on projects, he
17 was removed from that position. And in another situation, the
18 OSB libraries, his ability to commit directly to the main
19 branches was removed.

20 Q. When approximately were these changes made?

21 A. It would have been around the time that he changed
22 branches.

23 Q. Who made them?

24 A. I did.

25 Q. Why did you make them?

K253SCH3

Weber - Direct

1 A. Josh checked out of OSB, and I was following standard
2 practices. He no longer needed access to OSB's projects.

3 Q. How did you make these changes?

4 A. I logged into the Atlassian system and changed them. I
5 don't know if I used my administrative credentials for this or
6 the fact that I was an admin for the projects themselves,
7 because I was a lead for a significant portion of them. But
8 most likely it was my administrative credentials.

9 Q. Did you tell the defendant before you changed his
10 privileges to these projects?

11 A. No.

12 Q. Why not?

13 A. I felt it didn't need to be communicated. He was going to
14 be working on new projects, I didn't think he would even access
15 the old ones.

16 Q. I want to talk about one of OSB's projects in particular.

17 A. Okay.

18 Q. Are you familiar with a project called OSB libraries?

19 A. Yes.

20 Q. What is OSB libraries?

21 A. OSB was often tasked with projects that had a very short
22 deadline to meet. Days, sometimes weeks. And to ensure that
23 we were able to meet these deadlines, we wanted to have some of
24 the basic components that we often wrote in a state that can be
25 readily used.

K253SCH3

Weber - Direct

1 Q. What does that mean?

2 A. So, I often like to say that EDG did eight things, we just
3 did it a thousand different ways. So, if we needed to collect
4 a file from a computer, we had code that would do that. And if
5 you needed to collect a file, you could just incorporate that
6 code. It was already tested. It was already, you know, well
7 written.

8 Q. Who created OSB libraries?

9 A. It was a branch effort.

10 Q. Were there some developers in particular who were more
11 involved?

12 A. Yes.

13 Q. Who?

14 A. Myself, Frank, and Josh were some of the major contributors
15 early on. Matt as well.

16 Q. When the defendant was a member of OSB, what were his
17 privileges on OSB libraries?

18 A. So, as one of the senior members of that project, he had
19 the ability to merge code into the main branch. And by that I
20 mean, anybody had the ability to contribute to the libraries.
21 But before that code could be used by others, you would have to
22 have it signed off by a certain number of developers, show it
23 was well tested. Once those check boxes were hit, myself,
24 Brett, Josh, or Matt would be able to click a button on the
25 Atlassian web page and merge it in.

K253SCH3

Weber - Direct

1 Q. Was the merging aspect of OSB libraries important to OSB
2 libraries?

3 A. Yes.

4 Q. Why?

5 A. Once it was merged into the master branch, anybody in OSB
6 would inherently trust that code.

7 Q. After the defendant left the branch OSB, did his privileges
8 change to OSB libraries?

9 A. Yes.

10 Q. How did they change?

11 A. He was no longer granted access to merge in, into the
12 master branch, but was allowed to contribute just the same as
13 anybody else in the rest of the division.

14 Q. How could he still contribute to OSB libraries?

15 A. There was a process that we had officially outlined. You
16 would create a separate branch of the code, you would make your
17 modifications, and then you would submit it to review.
18 Everybody followed this process, regardless of if you were in
19 OSB or not.

20 Q. After the defendant left OSB and went to RDB, his new
21 branch, did he maintain those privileges?

22 A. Yes, he did.

23 Q. Who changed the defendant's privileges to OSB libraries?

24 A. I did.

25 Q. After you changed the defendant's privileges to OSB

K253SCH3

Weber - Direct

1 libraries, did he approach you about it?

2 A. Yes, he did.

3 Q. When approximately did he approach you?

4 A. I believe it was shortly after the change. I don't
5 remember the date, though.

6 Q. What happened during that interaction?

7 A. He came up to me, asked what was going on. I informed him
8 since he was no longer a member of OSB, that it had been
9 decided that he would not have the ability to merge stuff into
10 master. He disagreed with that. At which point I directed him
11 to talk to Sean, my branch chief, his former branch chief.

12 Q. What was his demeanor like during this interaction?

13 A. During the first interaction, it -- it wasn't anything
14 special. Very normal.

15 Q. You said you told him to talk to Sean?

16 A. Yes.

17 Q. Again, who is Sean?

18 A. Sean was my branch chief, chief of OSB.

19 Q. Why did you tell him to talk to Sean?

20 A. As chief of OSB, all of the projects were owned by him, and
21 he was the one that had the say on what -- how things should be
22 set up.

23 Q. Did the defendant talk to Sean?

24 A. Yes, he did.

25 Q. How do you know that?

K253SCH3

Weber - Direct

1 A. I directed him to go talk to Sean. I saw him go into
2 Sean's office. And then he came back afterwards to talk to me
3 again.

4 Q. Could you hear the conversation he had with Sean?

5 A. No.

6 Q. After the defendant talked to Sean, did he come back to
7 you?

8 A. Yes.

9 Q. Did you talk to him again?

10 A. Yes.

11 Q. What did he say?

12 A. He told me that Sean had said that his access should be
13 returned, and that I should go and do it.

14 Q. How did you respond?

15 A. I told him that I would talk to Sean, because that was not
16 my understanding of the situation.

17 Q. Did he respond to that?

18 A. Yes. He told me that I might as well go and do it, because
19 it was going to happen one way or another.

20 Q. What did you understand the defendant to mean by that?

21 A. I took it as a threat.

22 Q. Why?

23 A. The "one way or another" seem very much like an ultimatum
24 that he was going to do things his way, regardless of what was
25 said.

K253SCH3

Weber - Direct

1 Q. Did you talk to Sean after speaking with the defendant?

2 A. Yes.

3 Q. After speaking with Sean, did you give the defendant his
4 administrative accesses back to OSB libraries?

5 A. No.

6 Q. Why not?

7 A. Sean disagreed with Josh's recollection of the
8 conversation, and said that Josh was not supposed to have those
9 accesses. He asked that I e-mail Josh explaining exactly how
10 things are meant to be.

11 Q. After you spoke to Sean, did you e-mail the defendant?

12 A. Yes, I did.

13 MR. LAROCHE: Ms. Hurst, can you please publish
14 Government Exhibit 1061. Then go to the first e-mail in this
15 chain. Just go up one more page first for a second. The from
16 line is at the bottom.

17 Q. Is that the e-mail you sent?

18 A. Yes, it is.

19 MR. LAROCHE: We can zoom out and go to the next page.

20 Q. When did you send this e-mail?

21 A. This would have been April 14, 2016.

22 Q. Was that on the same day that you had the conversation you
23 were just discussing?

24 A. Yes, it was.

25 Q. What time did you send it?

K253SCH3

Weber - Direct

1 A. 3:30 p.m.

2 Q. Who did you send it to?

3 A. I sent it to Josh.

4 Q. Who did you copy?

5 A. I copied Sean, chief of OSB, Tony, who was deputy division
6 chief for AED, Richard, and Frank.

7 Q. Who is Richard?

8 A. I don't know who Richard is.

9 Q. Who is Frank?

10 A. Frank was one of the main developers of the libraries.

11 Q. What was the subject line?

12 A. OSB libraries.

13 MR. LAROCHE: If we can zoom out. And then zoom in on
14 the text of the e-mail.

15 Q. If can you read the first line and the first bullet.

16 A. "Josh, I discussed things with Sean and this is the
17 situation."

18 Q. Then just the next bullet.

19 A. "In the short term, the OSB libraries remain an OSB project
20 and are under Frank Stedman and my guidance."

21 Q. What did you mean by under Frank Stedman and my guidance?

22 A. We would continue to lead the OSB libraries.

23 Q. Can you please read the next bullet.

24 A. "You are free to contribute to the libraries by creating a
25 branch and following the pull request model that is in place."

K253SCH3

Weber - Direct

1 Q. What did you mean by that?

2 A. This is the process that everybody followed to contribute
3 code to the libraries.

4 Q. Can you please read the next bullet.

5 A. "We are hoping to move the libraries to Kevin's authority
6 to make them officially an AED level resource."

7 Q. Who is Kevin?

8 A. He was the, he was the tech director for AED.

9 Q. What did you mean by "make them officially an AED level
10 resource"?

11 A. We felt that the libraries were a very good idea and could
12 be leveraged by other people in the division. And we wanted to
13 see it grow.

14 Q. Then please read the next bullet down.

15 A. "When Kevin takes over, and if he desires for you to have
16 direct authority for the two long lived branches, then we will
17 give you commit access to master and develop."

18 Q. What type of access were you talking about potentially
19 giving back?

20 A. This would be his ability to merge code into the master and
21 develop branches.

22 Q. What did you mean by "when Kevin takes over"?

23 A. We wanted to, again, make this Kevin's responsibility to
24 chart the direction of the libraries as well as maintain the
25 authenticity of the code. And so, we wanted -- it was in the

K253SCH3

Weber - Direct

1 works to have him become lead of the project.

2 Q. Please read the last sentence of the e-mail.

3 A. "Until something officially changed, you must follow the
4 pull request model and leave it to either Frank or me to
5 complete the merge."

6 Q. What did you mean by "you must follow the pull request
7 model"?

8 A. Again, we had a well-laid out process that anybody,
9 including Frank and myself, would follow for contributing code
10 to the main branches. You would write what you wanted to
11 change, and then you would put it up for review. Once enough
12 people reviewed it and felt it met quality thresholds, it would
13 be merged into the main branch.

14 Q. Just zoom out again. This e-mail was sent at 3:30 p.m., is
15 that correct?

16 A. That is correct.

17 MR. LAROCHE: Ms. Hurst, if you can go to the next
18 e-mail in this chain. Just zoom in on the to from.

19 Q. Who sent this e-mail?

20 A. Josh did.

21 Q. When did he send it?

22 A. He sent it on the same date, April 14, 2016, at 3:39 p.m.

23 Q. Did he copy all the same people that were on other e-mail?

24 A. Yes, he did. I don't know if Kevin was on the first
25 e-mail, technically.

K253SCH3

Weber - Direct

1 Q. If we can go to the text of this e-mail. Read the first
2 sentence, please.

3 A. "Hey guys, thanks for the e-mail. I know soon Richard will
4 relieve Sean of his official duties."

5 Now I remember who Richard is.

6 Q. Who is Richard?

7 A. Richard was a senior developer in OSB. Sean was moving on,
8 he accepted a new position, and Richard was going to take over
9 temporarily as chief of OSB.

10 Q. Can you read the next sentence.

11 A. "I've talked with Anthony and Sean a bit about working on
12 transitioning some of my old projects, but haven't specifically
13 talked about the OSB libraries until now."

14 Q. And the next sentence, please.

15 A. "Since the OSB libraries were initially my idea that
16 stemmed from Brutal Kangaroo, and I've spent a lot of time and
17 effort managing and helping administer them, I'd like to stay
18 on along with Frank and Jeremy as helping administering them."

19 Q. Were the OSB libraries the defendant's idea?

20 A. No.

21 Q. Whose idea were they?

22 A. It was primarily mine and Frank's.

23 Q. At the time he sent this e-mail, had you already had a
24 conversation with him about OSB libraries?

25 A. Yes. It was the conversation we just talked about.

K253SCH3

Weber - Direct

1 Q. Had he already had a conversation with Sean about OSB
2 libraries?

3 A. Yes.

4 Q. Can you read the next sentence, please.

5 A. "Especially considering that the goal is to move these to
6 AED and allow Kevin to admin them, I feel like my intimate
7 knowledge with the libraries would be beneficial to this
8 process."

9 Q. And next sentence.

10 A. "I believe I should still have sufficient time to help with
11 the libraries, and it would help propagate the libraries by
12 having people on other branches working together on them."

13 Q. And just skip to the last sentence that starts "so" at the
14 bottom.

15 A. "So if OSB and RDB would be okay with this, I would like to
16 continue my active role with the libraries."

17 Q. At the time he sent this e-mail, had you spoken to Sean
18 about the libraries?

19 A. Yes.

20 Q. What did Sean say about his accesses to the libraries?

21 MS. SHROFF: Objection as to hearsay.

22 THE COURT: Overruled.

23 A. Sean was completely okay with Josh contributing to the
24 libraries following the official process, but wanted Frank and
25 I to be the ones that managed merging stuff into master and

K253SCH3

Weber - Direct

1 develop until Kevin took over and made a decision on that.

2 Q. Had you communicated that with the defendant?

3 A. Yes.

4 MR. LAROCHE: You can pull this e-mail down.

5 Q. After the defendant sent this e-mail, what, if anything,
6 did you do with respect to OSB libraries?

7 A. I went back in and looked at the audit logs on the
8 libraries.

9 Q. What are audit logs?

10 A. Audit logs can be anything that contain information.
11 Specifically in this scenario, it was logs that said when
12 permissions were assigned, removed, changed; things like that.

13 Q. What, if anything, did you see in the audit logs with
14 respect to OSB libraries?

15 A. Following this e-mail, Josh changed the permissions to give
16 him access to the master and develop branches again.

17 Q. How do you know it was the defendant who changed the
18 project permissions to OSB libraries?

19 A. The change was done by Josh's Active Directory account,
20 which only he would have known the user name and password to.

21 Q. What privileges did the defendant use to change his
22 accesses to OSB libraries?

23 A. He used his administrative privileges on the Atlassian
24 products.

25 Q. Were the defendant's actions consistent with CIA policy?

K253SCH3

Weber - Direct

1 A. No, they were not.

2 MS. SHROFF: Objection.

3 THE COURT: Overruled.

4 Q. You can answer again.

5 A. No they were not.

6 Q. Was the defendant allowed to do this as an administrator of
7 the Atlassian services?

8 A. No, he was not.

9 Q. Why not?

10 A. You are given a lot of ability as an administrator, but
11 everything that we did would be at direction.

12 Q. Had the defendant ever done anything like this before?

13 A. No.

14 Q. Did you tell anyone about the defendant using his
15 administrative privileges to reinstate his access to OSB
16 libraries?

17 A. Yes.

18 Q. Who did you tell?

19 A. I immediately informed Sean.

20 Q. Why did you tell Sean?

21 A. He was my immediate leadership.

22 Q. Why did you tell him immediately?

23 A. Because I saw this as a breach of the security rules, and
24 that this was an abuse of Josh's administrative privileges.

25 Q. Was this an urgent issue in your view?

K253SCH3

Weber - Direct

1 A. Yes, it was.

2 Q. Why?

3 A. Josh showed that he was no longer somebody that could be
4 trusted with his administrative credentials. Because he was
5 willing to do what he wanted to, versus what he was told to do.

6 Q. Was that problematic for someplace like the CIA?

7 A. Yes.

8 Q. Why is that problematic in the CIA?

9 A. The CIA, we have access to a lot of very damaging
10 information. And the only way we are able to work with this
11 type of information is by being trusted to handle it
12 appropriately.

13 Q. After speaking with Sean, did you talk to anyone else about
14 this issue?

15 A. Yes.

16 Q. Who?

17 A. Anthony and I believe Mike.

18 Q. You said Anthony. What was Anthony's position?

19 A. Anthony was the deputy division chief, so he was Sean's
20 immediate supervisor.

21 Q. Who was Mike?

22 A. Mike was the deputy group chief.

23 Q. Let's pull up Government Exhibit 89. Let's start with
24 Mike. What was Mike's role within this organizational chart?

25 A. Mike was the deputy group chief for EDG. So he was Karen's

K253SCH3

Weber - Direct

1 second.

2 Q. What about Anthony?

3 A. Anthony was the deputy division chief for AED.

4 Q. Again, what about Sean, where did he sit?

5 A. Sean was chief of OSB.

6 Q. How often did you have interactions with someone at Mike's
7 level?

8 A. I was more often than others -- I would not interact with
9 him often on stuff like this. I had other positions where I
10 would occasionally advise group level management about
11 technical topics.

12 Q. On this issue in particular, can you describe your
13 conversations with those individuals?

14 A. I relayed the facts of what happened. And then I was asked
15 to leave.

16 Q. After that conversation occurred, were you asked to do
17 anything in the days that followed?

18 A. Yes.

19 Q. What were you asked to do?

20 A. I was asked to come in with MSB -- sorry. ISB at the time.
21 They, it had been decided that ISB would take over the
22 administrative role of the Atlassian products, and I was there
23 to assist them in doing that.

24 Q. What day of the week did you go in?

25 A. Saturday.

K253SCH3

Weber - Direct

1 Q. Is Saturday a typical day to work within your group?

2 A. No, it is not.

3 Q. Why did you go in on a Saturday for this issue?

4 A. Two reasons. One, there was going to be a downtime of the
5 Atlassian products. We did not want this downtime to interfere
6 with the daily activities of the software development team.
7 And two, we wanted to make sure that we could do this without
8 Josh's interference.

9 Q. Why did you want to make sure you could do it without
10 Josh's interference?

11 A. We didn't trust him to not interfere.

12 Q. Did anyone else work with you on that Saturday?

13 A. Yes.

14 Q. Who?

15 A. It would have been Dave and Tim.

16 Q. Who is Dave and Tim?

17 A. They were system administrators within ISB.

18 Q. Did you have any instructions about what you were supposed
19 to do that day?

20 A. Yes.

21 Q. What were you supposed to do that day?

22 A. I was there to answer questions that ISB might have, and
23 oversee the transfer of administrative privileges. I was
24 explicitly told not to do any of the modifications to the
25 Atlassian products myself. And then after ISB was finished, to

K253SCH3

Weber - Direct

1 check that I did not have administrative access anymore.

2 Q. What administrative privileges were being changed that day?

3 A. The access to the Atlassian products.

4 Q. Why were your privileges also being taken away that day?

5 A. Mike and Anthony wanted to make it such that ISB was the
6 only administrators.

7 Q. Why?

8 A. They felt it was time for ISB to take it over.

9 MS. SHROFF: Objection as to what they felt.

10 THE COURT: Overruled.

11 A. They felt that it was time ISB took this over. It was
12 something that we requested numerous times. And they wanted it
13 so that only ISB would be administration to make sure that
14 developers developed, and system administrators handled
15 administration.

16 MR. LAROCHE: If we can pull that exhibit down and put
17 up Government Exhibit 1251, please. Please zoom in on the ESXi
18 server.

19 Q. At the time in 2016, an ESXi server was running Confluence
20 and Bamboo?

21 A. Yes.

22 Q. Who did that server belong to?

23 A. OSB.

24 Q. Who was administering that server as of April 2016?

25 A. It would have been myself, Frank, Matt. Those individuals.

K253SCH3

Weber - Direct

1 Q. Was the plan on that Saturday to give ISB control over that
2 server?

3 A. No.

4 Q. Why not?

5 A. The plan was for ISB to have control over the Atlassian
6 services. The ESXi server that we're talking about here was
7 going to remain an OSB resource, so there was no reason for ISB
8 to take it over.

9 Q. Who was going to remain as a server administrator of that
10 server after your weekend work on a Saturday?

11 A. Members of OSB.

12 Q. What, if any, role did the defendant have at that time as a
13 server administrator of the OSB server?

14 A. None.

15 Q. Why not?

16 A. He was no longer a member of OSB.

17 Q. Let's focus on what you did on that Saturday. Do you
18 remember what day that was in April?

19 A. I believe it was April 16.

20 Q. So you said that part of what you were doing was making
21 changes to the administrative services of Atlassian, correct?

22 A. Yes.

23 Q. Before making those changes, did you do anything to the
24 system?

25 A. Yes.

K253SCH3

Weber - Direct

1 Q. What did you do?

2 A. MSB or ISB created a snapshot of the VMs before making the
3 changes.

4 Q. So we're looking at Government Exhibit 1251 and we're still
5 zoomed in on the ESXi server. What do you mean by create a
6 snapshot?

7 A. Any time you're going to make like a major modification to
8 the running state of a service, taking a snapshot gives you a
9 safety net. So, we created a backup of that state and time
10 before we made any modifications to it.

11 Q. Just looking at this screen. Was a snapshot created of
12 Confluence?

13 A. Yes.

14 Q. Was a separate snapshot created of Bamboo?

15 A. Yes.

16 Q. We can pull that down.

17 After the snapshots were created, how were the
18 administrative privileges of the Atlassian services actually
19 changed?

20 A. MSB followed multiple -- they changed them in multiple
21 areas. One, the primary ways that we had access, we, Josh and
22 I had access to the Atlassian products, was through our Active
23 Directory credentials. That -- the group that our accounts
24 were part of was an Atlassian user group. We were removed from
25 that and ISB added their members to that group.

K253SCH3

Weber - Direct

1 In addition to that, we followed -- essentially, a
2 guide that said if you are resetting access to a Linux
3 operating system, do this, this and this. It was reset the
4 route password, change out any SSH keys. I can't remember
5 beyond that.

6 Q. We talked about SSH keys earlier.

7 A. Yes.

8 Q. Was that one of the ways that you could log in as an
9 Atlassian administrator?

10 A. Yes.

11 Q. How did you change SSH keys?

12 A. In this scenario, we deleted any known keys on the system,
13 MSB generated new keys, and then added those to the system.

14 Q. And you said MSB. Is MSB just another name for ISB?

15 A. Yeah. Sorry. Around this time, they were renamed from ISB
16 to MSB.

17 Q. After the passwords, new passwords were generated, were you
18 provided access to those passwords?

19 A. No, I was not.

20 Q. Why not?

21 A. I was no longer an administrator of the Atlassian product,
22 so I was not authorized to have access to it.

23 Q. What about the new SSH keys?

24 A. The same. Same thing. I didn't have access and was not
25 allowed access.

K253SCH3

Weber - Direct

1 Q. Let's focus on the OSB ESXi server for a moment.

2 A. Yes.

3 Q. Did you take any steps on April 16 to change the privileges
4 on that server?

5 A. Yes.

6 Q. What did you do?

7 A. The server had a route privilege, it was a shared password.
8 I reset that password to something else.

9 Q. Why did you do that?

10 A. In the -- I was doing my due diligence. It was in OSB's
11 control. Josh knew the old server password, so I felt it was
12 right to change that password.

13 Q. After you changed that server password, what, if anything,
14 did you do to OSB's Confluence page?

15 A. I updated the Confluence page to reflect the new password.

16 Q. Who had access to that page?

17 A. Only members of OSB.

18 Q. Did the defendant at that time have access?

19 A. I don't believe so.

20 Q. If we can put up Government Exhibit 1251 just for a moment.
21 I just want to talk through what the end result of April 16
22 was. So I just want to start with the Atlassian services.

23 After the changes on April 16, 2016, who had
24 administrative control over the Atlassian services?

25 A. MSB, ISB.

K253SCH3

Weber - Direct

1 Q. Did you have control?

2 A. No, I did not.

3 Q. After April 16, 2016, did you have any administrative role
4 with respect to the Atlassian services?

5 A. No. Outside of technically there's things like project
6 admins, but that's outside of what would be traditionally
7 considered an administrator.

8 Q. What about the defendant? After April 16, 2016, did he
9 have any administrative role over the Atlassian services?

10 A. No.

11 Q. Let's talk about the ESXi server. If we can zoom in on
12 that on top left, please. After April 16, 2016, who had
13 administrative control over the ESXi server?

14 A. It should have been members of OSB.

15 Q. Did the defendant have any administrative role with respect
16 to that server?

17 A. I don't believe so.

18 Q. You stated that that server was used for things other than
19 running Confluence and Bamboo programs; is that right?

20 A. That's correct.

21 Q. Did that include work on other OSB projects?

22 A. Yes.

23 Q. After the defendant moved to RDB, are you aware of any need
24 for him to have access to that server for his projects?

25 A. No.

K253SCH3

Weber - Direct

1 Q. Did his new branch, RDB, use the ESXi server for any of its
2 projects?

3 A. I don't believe so. They would not have interacted with
4 the ESXi server directly. They might access a VM or two that
5 was on the system. But, not the ESXi server itself.

6 Q. We can pull that down. Thank you.

7 After April 16, 2016, were developers notified about
8 the change in administrative privileges on the DevLAN network?

9 A. I don't know. I believe so.

10 MR. LAROCHE: Let's look at Government Exhibit 1064.
11 Just zoom in on the top to from of this e-mail.

12 Q. When was this e-mail sent?

13 A. It would have been April 18, 2016.

14 Q. Who sent this e-mail?

15 A. Anthony.

16 Q. Who did he send it to?

17 A. All of AED, ISB, as well as James.

18 Q. And you see there is a BCC line?

19 A. Yes.

20 Q. What does BCC mean?

21 A. Blind carbon copy. Anybody who received this e-mail would
22 not see that Anthony and Michael were also on this line.

23 Q. Is that the same Michael you referred to as the deputy
24 chief of EDG?

25 A. That's correct.

K253SCH3

Weber - Direct

1 Q. What was the subject of this e-mail?

2 A. "Update to Atlassian products admins."

3 MR. LAROCHE: If we can just zoom out and zoom in on
4 the second paragraph.

5 Q. Can you just read the first sentence.

6 A. "Following updates and changes to our -- blank -- internet
7 system, EDG has begun to take look at our other networks to get
8 a better understanding of our policies, etc. After a brief
9 DevLAN audit, we realized we never quite finished transitioning
10 the Atlassian products to SED/ISB for administration updates,
11 etc. Therefore, to ensure that everyone in EDG was not
12 affected while this transition was being made, SED/ISB
13 personnel transferred all system admin responsibilities across
14 all Atlassian products to SED/ISB removing local admin rights
15 for all local AED branch system admins this past weekend."

16 Q. Was this summarizing the work you did on April 16?

17 A. Yes.

18 Q. If we can zoom in on the next paragraph, please. Just read
19 the first sentence.

20 A. "As a result of this change, there are now two people in
21 SED/ISB who will maintain and update the Atlassian suite
22 repository for EDG."

23 Q. Was the defendant one of those two people?

24 A. No, he was not.

25 Q. Who were?

K253SCH3

Weber - Direct

1 A. It would have been Dave and Tim.

2 Q. Can you read the next sentence, please.

3 A. "This will ensure that our entire CNE library of tools,
4 code repository, etc. is backed up regularly. Updates to the
5 Atlassian tool suite are scheduled and maintained, and the
6 library remains under a common source control authority in
7 ISB."

8 Q. There a reference to being backed up regularly.

9 A. Yes.

10 Q. What's that a reference to?

11 A. This is the backups that we discussed earlier.

12 Q. After April 16, 2016, did the defendant have any role
13 administering the backups?

14 A. No, he did not.

15 Q. We can pull that down. That e-mail was sent on April 18,
16 2016?

17 A. Yes.

18 Q. As of that date, was the ESXi server still running
19 Confluence and Bamboo?

20 A. Yes, it was.

21 Q. Did that change?

22 A. Yes, it did.

23 MR. LAROCHE: Can we publish Government Exhibit 1067,
24 please. Just zoom in on the to from at the top, please.

25 Q. What's the date of this e-mail?

K253SCH3

Weber - Direct

1 A. This would be April 20, 2016.

2 Q. What time was this e-mail sent?

3 A. 12:06 p.m.

4 Q. Who sent it?

5 A. I did.

6 Q. Who did you send it to?

7 A. All of EDG, staff and contractors.

8 Q. Would EDG staff include the defendant?

9 A. Yes, it would.

10 Q. What's subject of this?

11 A. "Scheduled downtime for Bamboo and Confluence 4/25/2016."

12 Q. If we can just zoom in on the text of the e-mail. Just
13 read that into the record, please.

14 A. "All, on Monday, April 25 at 6 a.m., ISB will be migrating
15 the Bamboo and Confluence servers to new hardware and will need
16 to power them down for a limited amount of time. To ensure no
17 work is lost, please log out of Confluence and Bamboo when you
18 depart on Friday. If this maintenance window will cause any
19 issues for you, feel free to contact me."

20 Q. Can you summarize what you meant in this paragraph.

21 A. So, I was asking everybody to log out of the system, so
22 that there wasn't any unsaved work before ISB powered off the
23 machines.

24 Q. Why were they going to power off machines?

25 A. They were going to be transitioned to new hardware off of

K253SCH3

Weber - Direct

1 OSB's ESXi server.

2 Q. So Confluence and Bamboo would no longer being running on
3 the OSB server?

4 A. That's correct.

5 MR. LAROCHE: We can pull that e-mail down, please,
6 and pull up Government Exhibit 1069. Then just please zoom in
7 on top, the to from.

8 Q. When was this e-mail sent?

9 A. This would have been April 20, 2016, at 3:58 p.m.

10 Q. Who sent it?

11 A. Robert.

12 Q. Who did he send it to?

13 A. To the EDG group, as well as ISB.

14 Q. Would the defendant have received this e-mail?

15 A. Yes, he would have.

16 Q. What's the subject?

17 A. "Atlassian suite maintenance, Monday, 25 April, 0600 to
18 1000 hours."

19 Q. If we can now just zoom in on the text of the e-mail,
20 please. Just read the first two paragraphs to start.

21 A. Okay. "Good afternoon. On Monday, 25 April, from 0600 to
22 1000 hours, the Atlassian suite, in particular, the Bamboo and
23 Confluence servers, will be unavailable due to maintenance.
24 SED/ISB will be transferring data to new servers/hardware to
25 bring DevLAN Atlassian suite under SED/ISB configuration

K253SCH3

Weber - Direct

1 management in accordance with EDG best practices."

2 Q. Can you summarize what those two sentences are saying.

3 A. That from 6 a.m. until 10 a.m., on 25 April, the Confluence
4 and Bamboo VMs were going to be transferred off of OSB's
5 infrastructure on to ISB's infrastructure.

6 Q. Is that the same information you had communicated earlier
7 in the day?

8 A. Yes, it was. I think a little bit more detailed on the
9 times.

10 Q. This is on April 20, 2016?

11 A. Yes.

12 MR. LAROCHE: If we can zoom in on the date, please.

13 A. Yes, April 20.

14 MR. LAROCHE: We can pull that down.

15 Your Honor, with the Court's permission can I read a
16 stipulation?

17 THE COURT: Yes.

18 MR. LAROCHE: It is hereby stipulated and agreed by
19 and among the United States of America, by Geoffrey S. Berman,
20 United States Attorney for the Southern District of New York,
21 David W. Denton Jr., Sidhardha Kamaraju, and Matthew Laroche,
22 Assistant United States Attorneys, of counsel, and Joshua Adam
23 Schulte, the defendant, by and with the consent of his counsel
24 Sabrina Shroff, Esq., Edward Zas, Esq., and James Branden,
25 Esq., that:

K253SCH3

Weber - Direct

1 If called as a witness, a member of the Federal Bureau
2 of Investigation or FBI computer analysis response team, this
3 person known as CART Member-1, with knowledge of the matter
4 would testify that on or about March 10, 2017, CART Member-1
5 was present at the office building for the Central Intelligence
6 Agency or CIA Center for Cyber Intelligence, or CCI, located in
7 the Washington Metropolitan area, the building known as the CCI
8 building. While CART Member-1 was present in room 9E79 of the
9 CCI building, CART Member-1 recovered (i) a Dell Precision
10 computer tower that was used by the defendant to access the CIA
11 computer network called DevLAN while the defendant was employed
12 at the CIA and that was logged into evidence as
13 E0001_RM9E79_FM014_tower. Known as device E0001. And (ii) a
14 Sandisk Extreme USB device that was logged into evidence as
15 E0003_RM9E79_FM014, known as device E0003_FM014. Device E0001
16 contained four hard drives, Hard Drive-1 through Hard Drive-4.
17 Government Exhibit 1201 is a compact disc containing true and
18 accurate copies of photographs of device E0001; Government
19 Exhibit 1202 is a compact disc containing true and accurate
20 copies of forensic files data recovered from Hard Drive-1;
21 Government Exhibit 1203 is a CD containing true and accurate
22 copy of forensic files and data recovered from Hard Drive-3;
23 government Exhibit 1203-28 is a CD containing a true and
24 accurate copy of a log file recovered from Hard Drive-3.
25 Government Exhibit 1204 is a compact disc containing true and

K253SCH3

Weber - Direct

1 accurate copies of photographs of device E0003_FM014; and
2 Government Exhibit 1205 is a compact disc containing true and
3 accurate copies of forensic files and data recovered from
4 device 0003_FM014.

5 If called as a witness, another member of FBI CART
6 known as CART Member-2 with knowledge of the matter would
7 testify that on or about March 11, 2017, while CART Member-2
8 was present in room 9E79 of the CCI building, CART Member-2
9 recovered a NetApp server containing 24 hard drives that was
10 logged into evidence as E0018_RM9E79_24HDD, known as device
11 E0018. Government Exhibit 1206 is a compact disc containing
12 true and accurate copies of photographs of device E0018, and
13 Government Exhibit 1207 is a compact disc containing true and
14 accurate copies of forensic files and data recovered from
15 device E0018.

16 If called as a witness, another member of FBI CART
17 known as CART Member-3 with knowledge of this matter would
18 testify that on or about March 23, 2017, while CART Member-3
19 was present in room 9W89A of the CCI building, CART Member-3
20 recovered an ESXi server that was logged into evidence as
21 E022_RM9W89A_Dell known as device E0022. Government Exhibit
22 1208 is a compact disc containing true and accurate copies of
23 photographs of device E0022, and Government Exhibit 1209 is a
24 compact disc containing true and accurate copies of forensic
25 files and data recovered from device E0022.

K253SCH3

Weber - Direct

1 If called as a witness, another member of FBI CART,
2 Member-4, with knowledge of the matter would testify that on or
3 about June 9, 2017, while CART Member-4 was present in room
4 9E78 of the CCI building, CART Member-4 recovered a Dell
5 Precision tower 7910 containing two hard drives that was logged
6 into evidence as E0056_RM9E78_010, also known as device E0056.
7 Government Exhibit 1210 is a compact disc containing true and
8 accurate copies of photographs of device E0056, and Government
9 Exhibit 1211 is a compact disc containing true and accurate
10 copies of forensic files data recovered from device E0056.

11 Finally, if called as a witness, another member of FBI
12 CART, CART Member-5, with knowledge of the matter would testify
13 that on or about March 12, 2017, while CART Member-5 was
14 present at an offsite CIA facility located in the Washington
15 Metropolitan area, CART Member-5 recovered a NetApp server that
16 was logged into evidence as E0012_RMLE70E, also known as device
17 E00012. Government Exhibit 1212 is a compact disc containing
18 true and accurate copies of forensic files data recovered from
19 device E0012.

20 It is further stipulated and agreed that this
21 stipulation, as Government Exhibit 3005, Government Exhibits
22 1201 through 1212, and all government exhibits identified on
23 this document may be received in evidence as government
24 exhibits at trial. Signed by the parties.

25 THE COURT: They're received in evidence.

1 MR. LAROCHE: Thank you, your Honor.

2 (Government's Exhibit 3005, 1201-1212, and all
3 exhibits contained therein received in evidence)

4 MR. LAROCHE: Your Honor, if the Court is close to a
5 break, this might be a good time to stop.

6 THE COURT: All right. We'll take a break now and
7 we'll resume at 1:30.

8 (Jury excused)

9 THE COURT: See you at 1:30.

10 (Recess)

11 (Continued on next page)

12

13

14

15

16

17

18

19

20

21

22

23

24

25

K25Wsch4

Weber - Direct

AFTERNOON SESSION

1:35 p.m.

THE COURT: Good afternoon. Please be seated.

(Jury present)

THE COURT: Please be seated.

Mr. Laroche.

MR. LAROCHE: Thank you, your Honor.

Ms. Hurst, can you please publish Government Exhibit 1251.

Q. Mr. Weber, before the break, we were talking about some of the privilege changes that occurred on April 16, 2016. Do you recall that?

A. Yes.

Q. I think one of the privilege changes you recalled was the Atlassian server administrators were changed after April 16, 2016, is that right?

A. That's correct.

Q. But just you and OSB remained in control of the ESXi server, is that correct?

A. That is correct.

MR. LAROCHE: Ms. Hurst, can you just zoom in on the ESXi server.

Q. After those changes were made on April 16, 2016, were Confluence and Bamboo still being run on the OSB ESXi server?

A. Yes.

K25Wsch4

Weber - Direct

1 Q. Were they being run as virtual machines?

2 A. Yes, they were.

3 Q. As a server administrator of the ESXi server, what types of
4 things could you do with a virtual machine running on a server?

5 A. You could power the machine on, power it off. You could
6 delete it. You could take a snapshot. You can revert to a
7 snapshot, things like that.

8 Q. And the snapshot is the same thing you were talking about
9 earlier, which is something you created on April 16, 2016, is
10 that right?

11 A. That's correct.

12 Q. And what did you create snapshots of that day?

13 A. We created snapshots of Confluence and Bamboo.

14 Q. What were the purposes of those April 16 snapshots of
15 Confluence and Bamboo?

16 A. If we messed up the changes that we were making to the
17 system, we wanted a point in time that we could revert back to
18 to undo those changes.

19 Q. And just focusing on what those snapshots would have
20 contained, what administrative privileges would have been
21 contained within those snapshots?

22 A. So, the snapshot would have had the setup as it was before
23 we made the change. So I would have had admin access, Josh
24 would have had admin access. And we'd revert it back to that.

25 Q. And you talked about earlier access to the backups, is that

K25Wsch4

Weber - Direct

1 correct?

2 A. Yes.

3 Q. And one of the things you talked about were the mount
4 points?

5 A. Correct.

6 Q. And the mount points the defendant set up?

7 A. Yes.

8 Q. Where would those mount points have been?

9 A. They would have been in each of those VMs, the Confluence
10 VM, the Bamboo VM.

11 Q. What access did you need to get to those mount points?

12 A. You would have needed to log in to the host operating
13 system, which would have required access to the admin account
14 on the host operating system.

15 Q. And were those accesses in place for the defendant prior to
16 the changes on April 16, 2016?

17 A. Yes.

18 MR. LAROCHE: Let's go back to Government Exhibit
19 1069.

20 Q. We talked about this email also before the break, is that
21 correct?

22 A. Yes, we did.

23 Q. When was this email sent?

24 A. This email was sent on April 20, 2016, at 3:58 p.m.

25 Q. What changes were going to be made on April 25, 2016?

K25Wsch4

Weber - Direct

1 A. The machines, Confluence and Bamboo, were going to be
2 transferred to the new infrastructure.

3 Q. So the virtual machines that were running on the OSB server
4 were getting transferred to another server?

5 A. That is correct.

6 Q. I want to show you some log files that have been entered
7 into evidence from the defendant's computer.

8 A. OK.

9 MR. LAROCHE: Please publish Government Exhibit
10 1202-18, a log file from the defendant's DevLAN computer.

11 Q. We're going to drill down on this, but do you recognize
12 what this is?

13 A. Yes, I do.

14 Q. What is it?

15 A. This is a log file that would have been generated by
16 VMware.

17 Q. And what is that?

18 A. VMware was the company that -- they owned ESXi. They did
19 vSphere. They did vCenter. So it's any one of those products.

20 Q. Generally speaking, what's a log file?

21 A. A log file is diagnostic information, historical
22 information. There's different types of log files.

23 Q. What do log files show?

24 A. Depending on the log file, a security log file would show
25 when somebody accessed certain information. You might have a

K25Wsch4

Weber - Direct

1 service log file that would aid you in diagnosing, like,
2 something was failing. It could be any manner of information.

3 Q. What does a VMware log file show?

4 A. In this case, an action that occurred on a VM.

5 MR. LAROCHE: Let's zoom in to the first three lines
6 of the highlighted text there. That's fine.

7 Q. Let's start on the first line. There is a "ShowWarn:M."
8 Do you know what that means?

9 A. That would have been the fact that it was showing a
10 warning, and I don't know what the colon M means.

11 Q. What about what's next to that?

12 A. That's a time stamp.

13 Q. What is the time stamp of this log file?

14 A. It's April 20, 2016, at 5:35 p.m.

15 Q. And then let's go to the right of the time stamp. There's
16 a confirm and then a colon. Could you please read that?

17 A. "Current state of the virtual machine will be lost unless
18 it has been saved in a snapshot. Revert to snapshot
19 BK4-16-2016."

20 Q. What is this log file showing?

21 A. This is a warning that would have been presented saying
22 that if the virtual machine is reverted to this snapshot,
23 any -- any work that had been done since that time stamp -- or
24 that date would have been lost.

25 Q. And then after the warning, it says revert to snapshot. Do

K25Wsch4

Weber - Direct

1 you see that?

2 A. Yes.

3 Q. What's that mean?

4 A. The -- I'm sorry. Could you repeat the question?

5 Q. Sure. On the first line, at the end, it says revert to
6 snapshot?

7 A. Yes.

8 Q. What does that mean?

9 A. That is telling the virtual machine to restore its state to
10 the snapshot that was taken.

11 Q. And then after that there's BK4-16-2016?

12 A. Yes.

13 Q. Do you know what that refers to?

14 A. BK is just a, what was decided to just be used as the name.
15 And the 4-16-2016 was also included in that name.

16 Q. Do you understand what's that referring to, though?

17 A. We're saying backup 4-16-2016. We're saying, just letting
18 anybody know who looked at the snapshot that this was taken at
19 this time.

20 Q. Is that a specific snapshot?

21 A. It is the one that we took the morning of 4/16 before going
22 and making the changes.

23 Q. So while the old administrative changes were still in
24 place?

25 A. That's correct.

K25Wsch4

Weber - Direct

1 Q. Do you know what server this is from?

2 A. Yes, I do.

3 Q. How do you know that?

4 A. The next line afterwards references OSB.DevLAN.net.

5 Q. And where is that?

6 A. It's on the second or third, depending on how you're
7 counting it, line, the one that starts with "VI client soap
8 tran:M."

9 Q. And at the end there's OSB.DevLAN.net?

10 A. That's correct.

11 Q. Could you just circle that, please.

12 What server that is?

13 A. That is OSB's ESXi server.

14 Q. What activity is this log file reflecting?

15 A. This is showing that the virtual machine that was sitting
16 on OSB's ESXi server was reverted to a snapshot at the time I
17 referenced earlier.

18 Q. Which virtual machine?

19 A. I don't know the specific virtual machine. I believe it
20 is -- I think in this position that I see, I don't think I see
21 anything that references the specific virtual machine. This
22 would have been Confluence or Bamboo, though.

23 Q. And why do you say Confluence or Bamboo?

24 A. Those were the two virtual machines that we worked with on
25 4/16.

K25Wsch4

Weber - Direct

1 Q. And what time did this activity occur?

2 A. This occurred on April 20 at 5:35 p.m.

3 Q. On April 20 at 5:35 p.m., did you revert a snapshot of
4 Confluence or Bamboo?

5 A. No, I did not.

6 Q. Is reverting a snapshot of Confluence or Bamboo an
7 administrative activity or a user activity?

8 A. It's an administrative activity.

9 Q. What privileges would be required to do that?

10 A. You would need to have a specific administrative privilege
11 to revert to, revert to snapshot.

12 Q. And is that server-level privileges?

13 A. It would have been an ESXi set of privileges, so it's for
14 the ESXi server.

15 MR. LAROCHE: You can take that down.

16 Q. I want to show you a file that comes from the NetApp
17 server.

18 MR. LAROCHE: Please publish Government Exhibit
19 1207-27.

20 Q. Do you recognize this?

21 A. Yes, I do.

22 Q. What is it?

23 A. This is a directory list of the Confluence directory and
24 the Altabackup.

25 MR. LAROCHE: If we could just zoom in on maybe the

K25Wsch4

Weber - Direct

1 top five or six lines, including the title of the columns.

2 Q. Let's just walk through the first few lines. Just starting
3 with -- first, where are these files located?

4 A. They're located in Altabackup.

5 Q. And just starting with the first column, what's the name?

6 A. The name is the -- it's Confluence_db20160201-0625.

7 Q. What TYPE of file is that?

8 A. It's a SQL file.

9 Q. What is that?

10 A. This -- SQL is a technology Confluence -- all of the data
11 that Confluence stored was in a SQL directory.

12 Q. Do you see the next column that says date modified?

13 A. Yes.

14 Q. What does that reflect?

15 A. Date modified is any time a file-write activity occurred,
16 so either the creation of this file the first time or a
17 modification to the file itself.

18 Q. So just looking at these two files, when were they created?

19 A. They were created on the 1st and the 2nd around 6:30 in the
20 morning.

21 Q. And then the next column says type. What is that?

22 A. Type is just a friendly explanation of the extension.

23 Q. And then the next column has size. What's that?

24 A. That is the size of the file on disk.

25 Q. The next column has date accessed. What does that reflect?

K25Wsch4

Weber - Direct

1 A. So, date accessed is anytime there was a read operation.
2 This would be opening the file to view it or copying the file.

3 Q. And the next column has date created. What's that?

4 A. So, date created is the date -- the first date that that
5 file was created on disk.

6 MR. LAROCHE: Can we zoom out again, please.

7 Ms. Hurst, if you can, please zoom in on the rows that
8 encompass government exhibit and also keep the top rows, if we
9 can. OK.

10 Q. Just focusing on the bottom for a moment, what is the
11 bottom showing?

12 A. Additional files in the directory, same information that we
13 just went over.

14 Q. Then there's a date modified that seems to be daily making
15 new backups, is that right?

16 A. Yes.

17 Q. I want you to focus on the backup that was modified on
18 March 3, 2016. Do you see that?

19 A. Yes, I do.

20 Q. Could you just circle that.

21 When was the backup that was created on March 3, 2016,
22 modified?

23 A. It was modified at 6:29 a.m. on March 3, 2016.

24 Q. Let's go to the date accessed. When was the backup created
25 on March 3, 2016, last accessed?

K25Wsch4

Weber - Direct

1 A. It would have been April 20, 2016, at 5:42 p.m.

2 Q. What types of actions would change the date accessed?

3 A. Opening the file to read it or copying the file.

4 Q. On this page, do you see any other backups that have a
5 different date accessed than date modified?

6 A. No, I do not.

7 Q. Mr. Weber, did you access the March 3, 2016, backup on
8 April 20, 2016, at 5:43 p.m.?

9 A. No, I did not.

10 Q. Did you copy the March 3, 2016, backup on April 20, 2016,
11 at 5:43 p.m.?

12 A. No, I did not.

13 Q. Have you ever accessed any backup in the Altabackups?

14 A. The most I would have accessed the files in the Altabackup
15 share would be to navigate to a folder like this, see that the
16 files are getting created and using that as "backup's good" and
17 then moving on.

18 Q. Have you ever copied any of those files in the Altabackups?

19 A. No, I have not.

20 MR. LAROCHE: Could we go to Government Exhibit
21 1207-28, please.

22 I'm sorry. 1207-30.

23 Q. Do you recognize what's on this screen?

24 A. This also looks like a, the backup folder, the Confluence
25 directory.

K25Wsch4

Weber - Direct

1 Q. And what types of files are on this screen?

2 A. So, TGZ is a term for compressed, a compressed file a
3 lot -- most people recognize -- a dot-zip file is very similar
4 to what you see here.

5 Q. And what are the purposes of these TGZ folders in the
6 backups?

7 A. So, these TGZ files would be the compressed contents, so
8 everything that we just saw in the SQL stuff, or similar data,
9 would be compressed to save file space.

10 MR. LAROCHE: Let's zoom in on maybe the first five or
11 six rows, please.

12 Q. And again, can you circle the TGZ file that was modified on
13 March 3, 2016.

14 What was the date accessed of that file?

15 A. The date accessed was April 20, 2016, at 5:43 p.m.

16 Q. Did you access this file at that time?

17 A. No, I did not.

18 MR. LAROCHE: We can pull that down.

19 Ms. Hurst, can you please publish Government Exhibit
20 1203-29, another log file from the defendant's DevLAN computer.

21 Q. Do you recognize this?

22 A. Yes, I do.

23 Q. What is it?

24 A. This is the output of a command that was entered into a
25 terminal session.

K25Wsch4

Weber - Direct

1 Q. What's a command?

2 A. So, a command would be calling a program to execute on the
3 computer.

4 Q. And you said a terminal session?

5 A. Yes.

6 Q. What is a terminal session?

7 A. The -- it's a -- it's a specific mode where you are typing
8 in commands, very similar to the old DOS days, where you type
9 something in, you get text back. It is not a GUI interface
10 where you're clicking through.

11 MR. LAROCHE: Ms. Hurst, can you zoom in on the first
12 three lines that are highlighted at the top, please.

13 Q. Let's start with the first line. It says root@OSB. What
14 does that mean?

15 A. That signifies that via SSH you logged in as the root user
16 on the OSB server.

17 Q. And next to root@OSB, what is VMFS?

18 A. In this case, it is a directory on the OSB server. It's a
19 folder that's used for VMware.

20 Q. What about volumes?

21 A. Again, it's another folder that's just descriptive for the
22 information that's held in it.

23 Q. And the long number and letters after that?

24 A. This would have been a unique identifier for a specific VM,
25 I think.

K25Wsch4

Weber - Direct

1 Q. And next to that there's an LS. Do you see that at the end
2 of the line?

3 A. Yes.

4 Q. What is LS?

5 A. LS is a command in Linux to list everything that is in a
6 directory.

7 Q. And do you see the dash ALTR?

8 A. Yes, I do.

9 Q. Do you know what that means?

10 A. I don't know all of the flags that are on this, but those
11 flags tell LS what information you are looking for.

12 Q. And what does this command do, LS?

13 A. It gives you a list of files in a folder.

14 MR. LAROCHE: Let's zoom out again.

15 Q. What does the rest of this page reflect?

16 A. This is the output of LS. It's -- these are the files that
17 were in that folder that was requested.

18 MR. LAROCHE: Could we go to the next page. And if we
19 can zoom in on the last quarter or so of the page, please.

20 Q. Before the last line, what are you seeing on this page?

21 A. A collection of log files.

22 Q. And why were these log files displayed?

23 A. They were requested by the LS command.

24 Q. And do you see the last line of log file that is dash RW 1,
25 root, root and then a 653670 number?

K25Wsch4

Weber - Direct

1 A. Yes.

2 Q. What is that?

3 A. So, the -- this is the permissions that are assigned to the
4 file, who has access to this file, as well as the size of the
5 file.

6 Q. Is this file dated?

7 A. Yes, it is.

8 Q. What's the date?

9 A. The date in this was April 20 at 9:55 p.m.

10 Q. And do you see that some of the files before that have
11 different dates?

12 A. Yes.

13 Q. Why is that?

14 A. So, it's the date -- I don't know if this is the created or
15 modified date that we're looking at, but their time stamps are
16 slightly different.

17 MR. LAROCHE: Let's go to the last line of this log
18 file.

19 A. OK.

20 Q. There's another root@OSB. Do you see that?

21 A. Yes.

22 Q. And at the end, there is an RM VPXA.log? What does RM
23 mean?

24 A. It deletes a file.

25 Q. And what is VPXA.log?

K25Wsch4

Weber - Direct

1 A. It is a log file on this system.

2 MR. LAROCHE: Let's go to the next page, please, and
3 then zoom in on the highlighted text.

4 Q. What are you seeing here?

5 A. More deletions of log files.

6 Q. Is viewing log files an administrative activity or a user
7 activity?

8 A. Administrator activity.

9 Q. What privileges are required to do so?

10 A. You would need access to the location the log files are
11 kept.

12 Q. Would that be administrative access?

13 A. Yes.

14 Q. Did you delete any log files on April 20, 2016?

15 A. No, I did not.

16 Q. How long did you act as an administrator of the Atlassian
17 services?

18 A. I believe about a year and a half. I don't -- I don't know
19 for sure.

20 Q. How long did you act as an administrator for the ESXi
21 server?

22 A. Over the entire time we had that ESXi server.

23 Q. Over any of those times, did you ever delete log files?

24 A. No, I did not.

25 Q. Why not?

K25Wsch4

Weber - Direct

1 A. There was no good reason to.

2 Q. What do you mean by that?

3 A. Log files are there for a reason. They're to help us
4 identify problems and be able to correct them. They're
5 relatively small in size, so there's no reason to delete them.

6 MR. LAROCHE: You can pull that down.

7 Q. I want to switch gears a little bit and I'm going to show
8 you --

9 MR. LAROCHE: And Ms. Hurst, just for the witness, the
10 parties and the Court.

11 Q. -- what's been marked as Government Exhibit 801.

12 MR. LAROCHE: If you could go to the next page,
13 please, for the witness, and the final page.

14 Q. Do you recognize the handwriting in this document?

15 A. Yes, I do.

16 Q. Whose handwriting is it?

17 A. Josh Schulte's.

18 Q. How do you recognize that handwriting?

19 A. I spent a lot of my career trying to understand Josh's
20 handwriting.

21 MR. LAROCHE: Your Honor, the government offers
22 Exhibit 801 into evidence.

23 MS. SHROFF: Your Honor, may I have a minute?

24 THE COURT: Yes.

25 MS. SHROFF: Your Honor, we object to this document

K25Wsch4

Weber - Direct

1 coming in through this witness. The government has to connect
2 it, but this is not the appropriate witness for it to come in.

3 THE COURT: Mr. Laroche.

4 MR. LAROCHE: He recognized the document as his
5 handwriting. I think that's sufficient for authentication
6 purposes.

7 THE COURT: Overruled.

8 MS. SHROFF: That's not sufficient, your Honor.

9 THE COURT: The objection's overruled.

10 MR. LAROCHE: I'm sorry, your Honor. We were going to
11 offer this in evidence.

12 THE COURT: Received in evidence.

13 MR. LAROCHE: Thank you.

14 (Government Exhibit 801 received in evidence)

15 MR. LAROCHE: Can you please publish that to the jury.

16 Q. Now, do you have any idea when this document was created?

17 A. No, I do not.

18 MR. LAROCHE: Well, I just want to have you look at
19 some portions of the document.

20 First, at the top, please zoom in on the title.

21 Q. Can you read that, please?

22 A. Malware of the Mind.

23 Q. Do you have any idea what that's referring to?

24 A. No, I don't.

25 MR. LAROCHE: We can pull that down.

K25Wsch4

Weber - Direct

1 Please go to the third page and zoom in on the second
2 paragraph, please.

3 Q. Please take a moment and read that into the record.

4 A. "Which brings me to my next point. Do you know what my
5 specialty was at the CIA? Do you know what I did for fun?
6 Data hiding and crypto. I designed and wrote software to
7 conceal data in custom-designed file systems contained within
8 the drive's slack space or hidden partitions. I despise data.
9 I split data across files and file systems daily to conceal the
10 crypto. Analysis tools could never detect random or
11 pseudorandom data indicative of potential crypto. I designed
12 and wrote my own crypto. How better to fool buffoons like
13 forensic examiners and the FBI than to have custom software
14 that doesn't fit into their two-week class where they became
15 forensic experts. Make no mistake. I am an expert in data
16 hiding and cryptography with thousands of hours of experience
17 and among the top specialists in the world (or was). I mean,
18 how many?"

19 Q. You talked earlier about trade craft?

20 A. Yes.

21 Q. Do you see any trade craft in this paragraph?

22 MS. SHROFF: Objection.

23 A. Yes.

24 THE COURT: Overruled.

25 Q. What trade craft is contained in this paragraph?

K25Wsch4

Weber - Direct

1 A. His discussion about crypto, hiding data in, like, slack
2 space and hidden partitions. I believe that covers what was in
3 here.

4 Q. Why is that considered trade craft?

5 A. These are techniques that we use to hide data, exactly as
6 was stated in here.

7 Q. Is that trade craft classified?

8 A. Yes, it would be.

9 Q. Why?

10 A. In the giving -- acknowledging that this was a technique
11 that we used would help an adversary detect us on the system.

12 Q. Other than testifying today, have you ever spoken publicly
13 about this trade craft?

14 A. No, I have not.

15 Q. Why not?

16 A. It was classified information, and doing so would damage
17 our potential operations.

18 MR. LAROCHE: You can pull that down. Thank you.

19 Ms. Hurst, can you please publish just to the Court,
20 witness and parties Government Exhibit 806. And just go
21 through the next few pages.

22 Q. Mr. Weber, do you recognize the handwriting in this
23 document?

24 A. Yes, I do.

25 Q. Whose handwriting is it?

K25Wsch4

Weber - Direct

1 A. Josh Schulte's.

2 MR. LAROCHE: Your Honor, the government offers 806
3 into evidence.

4 MS. SHROFF: Your Honor, we have the same objection.

5 THE COURT: OK. Same ruling. Overruled.

6 Received in evidence.

7 MR. LAROCHE: Thank you, your Honor.

8 (Government Exhibit 806 received in evidence)

9 MR. LAROCHE: If we could go to the last page and then
10 publish it for the jury. And please just zoom in on the top
11 left date.

12 Q. Mr. Weber, can you please read that?

13 A. 7/14/18, Saturday.

14 MR. LAROCHE: And if we can zoom out and zoom in on
15 the text on the right.

16 Q. Can you please read that text, starting at the top?

17 A. "New attack plan.

18 "(1) FBI not the only agency against Trump. CIA too.

19 "(a) leak documents to make Trump look bad

20 "(b) sell documents to make money.

21 "(2) political dissent." I don't, I don't know if I can
22 read that word.

23 "(3) incompetence at the CIA, government agencies.

24 "(4) if I were Russia, I would blank

25 "(a) attack judiciary

K25Wsch4

Weber - Direct

1 "(b) U.S. destroy itself."

2 MR. LAROCHE: Thank you. We can pull that down.

3 Ms. Hurst, can you please show the witness, the
4 parties and the Court Government Exhibit 809 and just flip
5 through a few of the pages on this document for the witness,
6 please.

7 Q. Do you recognize this document?

8 A. Yes, I do.

9 Q. Do you recognize the handwriting in this document?

10 A. Yes, I do.

11 Q. Whose handwriting is it?

12 A. Josh Schulte's.

13 MR. LAROCHE: The government offers Government Exhibit
14 809 into evidence.

15 MS. SHROFF: Same objection, your Honor.

16 THE COURT: OK. 809's received in evidence.

17 (Government Exhibit 809 received in evidence)

18 MR. LAROCHE: Ms. Hurst, can you please go to page 9
19 and then publish it for the jury.

20 Ms. Hurst, can you please zoom in on the line that
21 starts "Twitter," in the middle of the page.

22 Q. Can you read that, Mr. Weber?

23 A. "Twitter: Free Jason Bourne."

24 Q. Who is Jason Bourne?

25 A. Jason Bourne was a fictional character in the Jason Bourne

K25Wsch4

Weber - Direct

1 movies.

2 Q. And what type of character was he?

3 A. He was a superagent for the CIA.

4 MR. LAROCHE: If we can zoom out, please.

5 Ms. Hurst, can you focus in on the next four lines
6 before free Jason Bourne -- or four lines below. Sorry.

7 Q. Can you read that, please?

8 A. "The @Department of Justice arrested the wrong man for
9 Vault 7. I personally know exactly what happened, as do many
10 others. Why are they covering it up?" And then "must be" or
11 "meet."

12 The bottom portion's cut off a little bit there.

13 MR. LAROCHE: Let's look at the remaining portion of
14 that page.

15 Q. Starting with the line that says "meet," in the middle
16 there, by your name --

17 A. "Meet the CIA's stir sack or struck Jeremy Weber and Karen.
18 You can find his info in the Ashley Madison dump at the CIA.
19 Set up Joshua Schulte. Jeremy Weber hacked Atlassian's Crowd
20 and when Schulte -- the admin found out, Karen issued him a
21 memo/letter of" -- the handwriting's difficult -- "a letter of
22 warning for self-granting admin privileges. The system
23 administrator self-granting admin privileges. Hmm. Right over
24 the FBI's head too. Or was it?"

25 Q. Just stop there for a second.

K25Wsch4

Weber - Direct

1 One of the things that's written by the defendant here is
2 Jeremy Weber and Karen set up Joshua Schulte. Did you set up
3 Joshua Schulte?

4 A. No, I did not.

5 Q. The defendant then writes, "Jeremy Weber hacked Atlassian's
6 Crowd." Do you have any idea what he's referring to there?

7 A. No.

8 Q. Did you ever hack Atlassian's Crowd?

9 A. No, I did not.

10 Q. Please read the bottom portion of this page.

11 A. "Schulte is the scapegoat because he routinely reported
12 security issues at the CIA, including infrastructure branches,
13 abysmal" -- management, maybe. I don't know the last word
14 there.

15 Q. Did the defendant routinely report security issues at the
16 CIA?

17 A. No, he did not.

18 MR. LAROCHE: Can we go to the next, page, please, and
19 just focus in on the top left quarter of this page.

20 A. "At USG, just to authenticate me first, the @CIA was
21 involved in blank. The code for initially planned cyber
22 operation is in Vault 7. Tool described in vendor report is,
23 in fact, Bartender, CIA tool set for operators to configure for
24 deployment."

25 Q. Are you familiar with Bartender?

K25Wsch4

Weber - Direct

1 A. Yes, I am.

2 Q. What is Bartender?

3 A. It is a tool that I worked on for an extent -- the majority
4 of my career in OSB.

5 Q. Generally speaking, what does that tool do?

6 A. The tool was meant to collect files from a computer via
7 thumb drive that an operator had access to.

8 Q. The defendant wrote that Bartender was described in a
9 vendor report?

10 A. Yes.

11 Q. Is that right?

12 A. Yes.

13 Q. Did the vendor report attribute that tool to the CIA?

14 A. No, it did not.

15 Q. Has the CIA ever acknowledged that that's a CIA tool?

16 A. No, it did not.

17 Q. Why not?

18 A. The attribution, especially in this scenario, would be very
19 concerning because operators were the ones that would start
20 this tool, and if it was caught, attribution could lead to the
21 capture of a CIA officer.

22 Q. Other than testifying today, have you ever discussed
23 Bartender publicly?

24 A. No, I have not.

25 Q. Why not?

K25Wsch4

Weber - Direct

1 A. It was classified information. Discussing it would put CIA
2 officers' lives at risk.

3 MR. LAROCHE: You can pull that down.

4 Q. Early in your testimony today, you talked about the March 7
5 leak?

6 A. Yes.

7 Q. I want to turn your attention back to that.

8 A. OK.

9 Q. One of the things you said was that the first leak, on
10 March 7, 2017, contained Confluence data, is that right?

11 A. That's correct.

12 Q. And that's Confluence data from DevLAN?

13 A. Yes.

14 Q. How much of Confluence was disclosed on March 7, 2017?

15 A. Everything up until a certain date.

16 Q. In what locations on DevLAN was all of the Confluence data
17 available?

18 A. It would have either been in the Confluence VM or in the
19 backups.

20 Q. I want to talk about a few documents that were disclosed by
21 WikiLeaks from that first initial leak.

22 A. OK.

23 MR. LAROCHE: Ms. Hurst, can you please publish
24 Government Exhibit 6 and zoom in on the text.

25 Q. Showing you a portion of the directory from the March 7

K25Wsch4

Weber - Direct

1 leak, do you recognize that?

2 A. Yes, I do.

3 Q. And what is this? What are these lines?

4 A. So, the first line, data transfer modules, was -- this was
5 a page on Confluence. Everything below that is subpages to
6 that that talked about specific ways that we would store data
7 for transfer.

8 Q. And can you read the third line?

9 A. Yes. "Transferring data using NTFS alternate data streams,
10 DG NTFS ADS BK Brutal Kangaroo."

11 MR. LAROCHE: Let's go to Government Exhibit 6-1,
12 please. If we could just zoom in on the middle, starting
13 "transferring data," including the banner.

14 Q. What is this page showing?

15 A. This page is a description of this specific technique.

16 Q. And does that connect to the last exhibit we saw in any
17 way?

18 A. Yes, it's -- if you had clicked that link, it would take
19 you to this page.

20 Q. And you said a specific technique. What were you referring
21 to there?

22 A. I mentioned earlier that EDG does eight things a thousand
23 different ways. One of those eight things is data --
24 transferring data. This technique is a way of -- one of the
25 many ways that we would store data and transfer it between a

K25Wsch4

Weber - Direct

1 target machine to a CIA infrastructure.

2 Q. Just focusing on the parentheses there, it starts DTN and
3 there's some more letters. Do those letters have any
4 significance?

5 A. Yes, they do.

6 Q. What significance?

7 A. The DT is an abbreviation for data transfer. NTFS ADS is
8 for NTFS alternate data streams, which is the technique, the
9 specific technique that's being used here. And BK is letting
10 other people know that this was originally designed for Brutal
11 Kangaroo.

12 Q. What is Brutal Kangaroo?

13 A. Brutal Kangaroo was a tool suite created by Josh Schulte.

14 Q. And then underneath this title, there's a secret/nofor
15 n banner?

16 A. Yes.

17 Q. Just remind us what that is.

18 A. The classification of this document was secret and should
19 not be shared with any foreigners.

20 Q. Was this one of the documents that was obtained from
21 Confluence?

22 A. Yes, it was.

23 Q. Was it common to post classification banners on Confluence?

24 A. Yes, usually it was. It wasn't a universal -- it wasn't a
25 universal thing, but it was something we often did.

K25Wsch4

Weber - Direct

1 Q. And why?

2 A. It helped so that we knew what type of page we are seeing.

3 MR. LAROCHE: We can zoom out again.

4 And then if we could go to Government Exhibit 6-2.

5 Q. Showing you another version of the previous exhibit, do you
6 see the same title there?

7 A. Yes.

8 MR. LAROCHE: If we could go down to page 2 and then
9 zoom in on the notes.

10 Q. Can you summarize what these notes are showing?

11 A. This explains how to use -- how to use the technique as
12 well as what information is in the technique so that you
13 could -- this is meant to help somebody implement this.

14 Q. You've talked about attribution before, attributing tools
15 to the CIA?

16 A. Yes.

17 Q. What, if any, impact would the disclosure of this
18 information have on attributing a tool to the CIA?

19 A. This is a pretty significant clue.

20 Q. Why?

21 A. It tells exactly how data at rest is stored. So if
22 somebody was doing a forensic review and saw a structure like
23 this as well as these types of commands, they now have
24 something that says this was a CIA tool.

25 MR. LAROCHE: We can pull that down.

K25Wsch4

Weber - Direct

1 Ms. Hurst, please publish Government Exhibit 11-2.

2 Q. What is this?

3 A. This is a, just a help page that was on Confluence.

4 MR. LAROCHE: And if we can just zoom in on the "wait"
5 and the banner for a second.

6 Q. Do you recognize this page at all?

7 A. Yes, I do.

8 Q. And why do you recognize it?

9 A. It was something that was on our Confluence and was
10 something that I would have read at some point.

11 MR. LAROCHE: And if we can go back out a second, just
12 to the wider one, and then zoom in on the first two paragraphs.

13 Q. Summarize what these paragraphs are describing.

14 A. So, the first paragraph is just talking about some history
15 of a previous, you know, previous deployment of a tool.

16 And the second part is talking about, talking about
17 attempting to overwrite a file that was written to obfuscate
18 our involvement and finding out that that file wasn't correctly
19 overwritten.

20 Q. Have you ever talked about this type of information
21 publicly before?

22 A. No, I have not.

23 Q. Why not?

24 A. This is all techniques and, in this scenario, would have
25 been a specific operation that we were supporting.

K25Wsch4

Weber - Direct

1 MR. LAROCHE: If we can go to Government Exhibit 15.

2 Q. Earlier today we showed you a user guide for Brutal
3 Kangaroo. Do you recall that?

4 A. Yes, I do.

5 Q. What part of the WikiLeaks disclosure did that document
6 come from?

7 A. I don't remember if that document was in Confluence or
8 Stash or both.

9 Q. Do you remember subsequent disclosures from Stash?

10 A. Yes.

11 Q. Is this one of the documents, Government Exhibit 15, that
12 came from Stash?

13 A. Yes.

14 Q. And what is this document?

15 A. This is a slide deck that was created for the delivery of
16 Emotional Simian version 2.0.

17 Q. Are you familiar with it?

18 A. Yes.

19 Q. How are you familiar with it?

20 A. I was the primary author.

21 Q. Generally speaking, what is Emotional Simian?

22 A. Emotional Simian was a thumb drive-collection tool that was
23 designed for a scenario where the owner of a thumb drive was
24 unwitting to the fact that he was spreading malware by moving
25 the thumb drive between machines.

K25Wsch4

Weber - Direct

1 Q. What do you mean by unwitting?

2 A. The target did not know that they were a CIA target, nor
3 did they know that there was a CIA operation occurring.

4 MR. LAROCHE: Let's go to page 3.

5 Q. We're now on a page that's titled requirements.

6 A. Yes.

7 Q. What is a requirements page?

8 A. Requirements -- this is a very high-level discussion of
9 what the tool is supposed to do.

10 Q. And what was this tool supposed to do?

11 A. In this case, provide access to downstream machines that
12 would otherwise be inaccessible via thumb drives inserted by
13 unwitting users.

14 Q. You said downstream machines?

15 A. Yes.

16 Q. What does that mean?

17 A. This is a term that we used in the agency. You're -- you
18 would have a point of presence on the network somewhere, access
19 to a computer. Downstream machines are further into the
20 network that we don't necessarily have access to yet.

21 MR. LAROCHE: Let's go to the next page, please.

22 Q. And this page is titled concept of operations?

23 A. Correct.

24 Q. What is a concept of operations?

25 A. This is a high-level description of how we imagine the

K25Wsch4

Weber - Direct

1 deployment of the tool would go.

2 Q. And do you recognize the page?

3 A. Yes.

4 Q. How do you recognize it?

5 A. I created it.

6 Q. If we could just look at the diagram there in the middle --

7 A. OK.

8 Q. -- can you summarize what that diagram is telling us?

9 A. This takes you through the steps that the deployment of
10 this tool would go through. It would start on a configuration
11 machine, something that the agency owned, to the primary host,
12 which is that initial foothold that I had mentioned earlier,
13 and then, via a USB drive, infect secondary targets downstream.

14 MR. LAROCHE: If we can go to the next page, page 5.

15 Q. This is titled capabilities and limitations?

16 A. Yes.

17 Q. What is this page showing?

18 A. So, this is explaining -- like, there's no tool that does
19 everything. So this was explaining what the tool did and
20 didn't do.

21 Q. Other than testifying today, have you ever spoken publicly
22 about Emotional Simian?

23 A. No.

24 Q. Why not?

25 A. There, again, it would expose our methods and allow for the

K25Wsch4

Weber - Direct

1 detection of this tool.

2 MR. LAROCHE: We can pull that down, please.

3 Q. Focusing you again on March 7, 2017, just to orient us a
4 bit, prior to that, what was your typical workday like?

5 A. Nine to five. You know, some days longer than others, but
6 it was traditionally an eight-hour day.

7 Q. Did that change after the leak?

8 A. Yes, it did.

9 Q. How did it change?

10 A. The most noticeable impact was in that first week I was
11 assigned to lead a team to assess what was in the leak and what
12 the damage was. That was -- for that week I often would work
13 until about 2 a.m., go home for a few hours and then be back at
14 work around 6 a.m. to make sure that I could brief -- brief
15 senior leadership about the status of our work.

16 Q. Why were you working those long hours?

17 A. We were -- we were in damage mode, like the house was
18 burning down, and we were trying to figure out what was going
19 on.

20 Q. You said you were working on a team?

21 A. Yes.

22 Q. How many people were working on that team with you?

23 A. I think it was about ten.

24 We took one or two of the most senior developers in each of
25 the branches in AED, and they were assigned to me to make

K25Wsch4

Weber - Direct

1 assessments of what was in the leak.

2 Q. What were some of the things you were doing on that team?

3 A. There were three major focuses.

4 One was understanding what all had leaked out.

5 The second was looking for the biggest, like, "oh, crap"
6 disclosures, that if we saw this we need to inform people
7 immediately, because there's significant problems.

8 And third, we were looking for any information -- in
9 addition to the leak, WikiLeaks published an editorial. We
10 were reading through that editorial and seeing if they
11 referenced any information that wasn't in the leak to see if
12 there was any proof that they had additional information.

13 Q. Now, at the time of the leak, you had been at the agency
14 for how long?

15 A. I think close to seven years at that point.

16 Q. And during that time, you'd worked exclusively as a
17 developer developing cyber tools?

18 A. No.

19 Q. What else did you do?

20 A. A few months prior to the leak, I had become a branch chief
21 for one of the other branches in the division.

22 Q. Did that branch also develop cyber tools?

23 A. Yes, it did.

24 Q. During that time that you were at the CIA, what impact, if
25 any, did the public disclosure by WikiLeaks have on your past

K25Wsch4

Weber - Cross

1 work?

2 A. So, the public disclosure of my past work pretty much meant
3 all of that work was now no longer operationally useable. It
4 was dead.

5 Q. Why?

6 A. The risk of attribution to the CIA as well as the amount of
7 information that adversaries would have for detecting our
8 operations was too high, and we needed to rewrite that work.

9 MR. LAROCHE: No further questions, your Honor.

10 THE COURT: Ms. Shroff.

11 CROSS-EXAMINATION

12 BY MS. SHROFF:

13 Q. Good afternoon, Mr. Weber.

14 A. Good afternoon.

15 Q. Mr. Weber, you testified that you've worked at the CIA for
16 about seven years, is that correct?

17 A. No, that's not correct.

18 Q. I'm sorry. Could you correct me then?

19 A. It was close to ten years.

20 Q. You've been at the CIA for close to ten years?

21 A. That's correct.

22 Q. And I have it right, do I not, that you started at the CIA
23 before Mr. Schulte did? Correct?

24 A. I started full time before Joshua became a full-time
25 officer. He did internship tours shortly before I started full

K25Wsch4

Weber - Cross

1 time.

2 Q. So when you and Mr. Schulte worked together, were you both
3 essentially at the same level?

4 A. I was a little bit ahead of him in grade, but we were
5 close.

6 Q. And what would your title be at that time?

7 A. Developer would be the official title.

8 Q. And Mr. Schulte was also a developer, correct?

9 A. Yes.

10 Q. And you worked, both of you worked in the same group. Do I
11 have the nomenclature correct?

12 A. Yes, same group.

13 Q. And what was that group? Remind me, please.

14 A. Engineering Development Group.

15 Q. And at that time, how many people worked in EDG?

16 A. In EDG, maybe 200. I don't know. I don't know the number.

17 (Continued on next page)

K253SCH5

Weber - Cross

1 Q. The supervisor for you and Mr. Schulte, your immediate
2 supervisor, was whom?

3 A. During what time?

4 Q. Well, let's stick with 2015 and 2016, the same time frame
5 that Mr. Laroche covered.

6 A. Then that would have been Sean.

7 Q. So, you were never Mr. Schulte's boss, correct?

8 A. No. Not in an official capacity.

9 Q. There's only one capacity in which you can be someone's
10 boss, right?

11 A. No, that's not correct.

12 Q. So, the CIA had such a loosey-goosey structure that you
13 could be somebody's unofficial boss?

14 A. There are two types of leadership positions in the agency.

15 Q. So did you -- are you saying there are two types of formal
16 leadership positions in the agency?

17 A. One is --

18 Q. No, no. Could you answer that question first?

19 A. Could you repeat it?

20 Q. Sure. I just wanted to make sure if I understood you
21 correctly that there are two types of leadership positions.

22 What does that mean, by the way, "leadership
23 position"?

24 A. Leadership position has a very broad, broad definition.

25 Q. So, I don't understand what it means. I have a boss. I

K253SCH5

Weber - Cross

1 don't know what a leadership thing is. Can you explain that?

2 A. So the agency, there's two types of leadership in the
3 agency. Your official, like, leadership, the branch chiefs,
4 things of that nature, have what we refer to as -- you have a
5 responsibility to officially review an officer's work, and
6 document that for the record.

7 There are a significant additional amount of leadership
8 positions like team leads or project leads that you might, you
9 might provide feedback to the branch chief, but you would not
10 have an official say in the documentation of like how good or
11 bad an officer was doing.

12 Q. Okay. But when you were assigned to be a team lead or a
13 project lead -- not just you, in particular, but a person --
14 somebody assigns an individual to be a team lead, correct?

15 A. Occasionally. Sometimes it is just a natural formation.
16 It depends.

17 Q. Okay. Let's talk about a project lead, or is that the same
18 thing?

19 A. A project lead is one of the categories, yes.

20 Q. So when there is a project or a tool, a group of people
21 work on it in the CIA; is that how it works?

22 A. Sometimes. Sometimes people will work on things by
23 themselves, but yes.

24 Q. All right. so let's talk about when there is a group
25 working on it, okay?

K253SCH5

Weber - Cross

1 A. Yes.

2 Q. And when there is a group working on it, you said that
3 there is either a natural team leader, or some boss assigned
4 somebody and says "you are the team leader." Correct?

5 A. Yes.

6 Q. And if somebody assigns a team leader, everybody knows that
7 that team leader is assigned, correct?

8 A. Yes.

9 Q. Okay. And if it's just somebody who assumes a leadership,
10 the other people don't have to follow that leadership. They
11 can say, well, you're not the the team leader. Correct?

12 A. No, that is not correct.

13 Q. So anybody can just become a team leader on a project?

14 A. We all had ownership of projects. And whoever owned a
15 project would be the natural leader of it.

16 Q. Right. But I'm trying to figure out this natural leader
17 concept. All I'm trying to figure out is if you didn't like
18 your natural leader, could you say, hey, you're not my natural
19 leader on a project or not?

20 A. You could say you're not my leader and no longer work on
21 the project.

22 Q. Or you could go to Sean and say, hey, this guy's not my
23 natural leader, correct?

24 A. That's correct.

25 Q. And then Sean would figure it out, correct?

K253SCH5

Weber - Cross

1 A. Yes.

2 Q. Right. And in your particular unit, Sean was the person
3 who would generally figure things out, right?

4 A. At the time we're talking about, yes.

5 Q. We're only going to talk about that time, so you don't have
6 to worry about that. Okay? If I pick a different time period,
7 I'll tell you, okay?

8 A. All right.

9 Q. So you testified about this time period and you said
10 basically EDG was a -- correct me if I'm wrong because I don't
11 have a transcript in front of me. Was a friendly, collegial
12 place, correct?

13 A. Yes.

14 Q. And is it fair to say that most of the people who worked in
15 EDG were men, or is that not correct? I don't know.

16 A. I can speak more to AED.

17 Q. I'm only talking about the group you worked with
18 Mr. Schulte, 2015 to 2016.

19 A. AED was below that group.

20 Q. Right.

21 A. So, AED, that's a fair statement. EDG as a whole, I don't
22 know. I don't know what the layout would have been.

23 Q. Okay. Let's just focus on your subgroup then. Mostly men
24 you would say?

25 A. It was predominantly male.

K253SCH5

Weber - Cross

1 Q. And about how many -- you remember the diagram that
2 Ms. Hurst showed you of the ninth floor. If you could just
3 pull it back up, please.

4 While she's pulling it up, you basically showed it was
5 cubicles in which all of you sat, correct?

6 A. Yes, that is correct.

7 Q. And you sat somewhere next to Amol, correct?

8 A. That is correct.

9 Q. And somewhere next to Mr. Schulte?

10 A. That is correct.

11 Q. And then who was the person in the fourth cubicle?

12 A. Like at an angle from me?

13 Q. Yeah.

14 A. That would have been Frank.

15 Q. Frank?

16 A. Yes.

17 Q. You testified basically that it was a collegial
18 environment?

19 A. We were friendly with each other, yes.

20 Q. Friendly with each other. All right. Part of this
21 friendliness included people playing with each other with Nerf
22 guns?

23 A. Some developers did that.

24 Q. And they weren't like these teeny little Nerf guns, right?
25 They were like real serious investment of big plastic Nerf

K253SCH5

Weber - Cross

1 guns; is that correct?

2 A. There were all manners, but yes, some of them were as you
3 described.

4 Q. How many Nerf guns do you think all together were in this
5 little cubicle area? Four, six, 10, 12?

6 A. In our cubicle area, if I recall correctly, only Josh and
7 one other person had Nerf guns.

8 Q. And then in the broader cubicle area, other people had Nerf
9 guns?

10 A. Across the floor, yes.

11 Q. Okay. And they shot Nerf -- whatever comes out, I don't
12 know, I don't play with Nerf guns. But whatever it is that
13 come out of the Nerf guns, they shot at each other?

14 A. Occasionally.

15 Q. It was more than occasionally, right?

16 A. I didn't take part in it, so I don't know.

17 Q. Amol took part in it in terms of being annoyed by it,
18 correct?

19 A. I don't remember actually.

20 Q. Really?

21 A. Yes.

22 Q. You don't remember Amol being annoyed by Mr. Schulte
23 shooting Nerf guns at him?

24 A. I remember Amol being annoyed by Mr. Schulte on occasion.

25 Q. That we know.

K253SCH5

Weber - Cross

1 A. I don't specifically -- if he ever expressed it about the
2 Nerf guns.

3 Q. Okay. Do you recall Amol being annoyed at the Nerf gun
4 darts coming at him, and he would take the darts and throw them
5 behind his own desk?

6 A. Actually, yes. I do remember that now.

7 Q. Okay. Do you recall Amol or Mr. Schulte taking stuff from
8 each other's desks and hiding it behind each other's back?

9 A. No, I do not.

10 Q. Do you recall a general sense of people teasing each other
11 about habits and appearances?

12 A. Habits, yes. Appearances, typically no.

13 Q. You don't remember Amol calling him a bald asshole?

14 A. I do recall that, yes.

15 Q. He actually used to call him bald asshole, right?

16 A. Yes.

17 Q. And there was a gentleman in that unit that had some kind
18 of unfortunate autoimmune disease. Do you recall that human
19 being? The person -- I just, I don't want to personally out
20 someone's health issues.

21 A. No, I don't remember an autoimmune disease, no.

22 Q. Do you remember Amol telling somebody that he was going to
23 drop dead anyway, and stop complaining about the pain he was
24 feeling?

25 A. No, I do not recall that.

K253SCH5

Weber - Cross

1 Q. You don't recall that. Do you remember being asked about
2 Amol saying that your wife's investment in her work-related
3 401(k) was a financially stupid thing to do?

4 A. No.

5 Q. Do you remember being interviewed on video about this
6 particular allegation and saying to that individual --

7 A. The allegation that you're referencing is incorrect.
8 Like --

9 Q. Why don't you tell us what the allegation was.

10 A. The allegation was that my wife was dumb. And that a
11 decision she made was dumb. I remember referencing an
12 allegation where Josh said that my wife was dumb.

13 Q. Okay. But Amol did call your wife's decision to invest in
14 a particular investment dumb, correct?

15 A. Yes.

16 Q. And he told you that he thought your wife's decision was
17 dumb. Correct?

18 A. Yes.

19 Q. And you replied, "Better to have a dumb decision and a
20 happy wife. I can live with that every single time," correct?

21 A. Very much so.

22 Q. Make sure you tell my husband that.

23 So, had Mr. Schulte just written that complaint more
24 carefully, you would have answered the complaint differently as
25 you did during your interview, correct?

K253SCH5

Weber - Cross

1 A. There is a wide difference in the allegation that he made
2 and what actually happened, so, if he had correctly stated what
3 had happened, I would have answered differently, correct.

4 Q. And it's fair to say that by the time these allegations
5 were discussed with you, you had long stopped liking
6 Mr. Schulte, right?

7 A. I can't remember -- yes, I think that is a fair statement.

8 Q. Now, Mr. Schulte was friends with people in his group and
9 friends with people who worked at the CIA, correct?

10 A. Yes.

11 Q. One of those friends was a man named Michael; is that
12 correct?

13 A. That's correct.

14 Q. And you knew Michael as well, correct?

15 A. Yes.

16 Q. And was he part of your group or was he part of a separate
17 group?

18 A. The Michael that was his friend was in our branch.

19 Q. It was in your branch, right?

20 A. Yes.

21 Q. And Michael and Mr. Schulte also fought, correct?

22 A. There was only one scenario that I recall of a fight
23 between the two of them.

24 Q. Right. When that fight occurred, the person who gossiped
25 the most about that fight was in fact Amol, correct?

K253SCH5

Weber - Cross

1 A. I don't know.

2 Q. You don't remember Amol sending texts to everyone saying,
3 hey, you would not believe what happened between Michael and
4 Josh?

5 A. No.

6 Q. He didn't send you that text?

7 A. I don't believe so.

8 Q. Okay. Suffice it to say that the saga between Amol and
9 Josh went on for quite some time, right?

10 A. I'm sorry. Can you repeat the question?

11 Q. Is it fair to say that the saga between Amol and Josh went
12 on for quite some time?

13 A. Yes. As I stated earlier, they didn't get along and from
14 the getgo. And it depends when you want to define a saga
15 beginning.

16 Q. Okay. Well there came a point when you defined when the
17 saga began, right?

18 A. Yes.

19 Q. Okay. And you said that, for you at least, the breaking
20 point was that you thought Mr. Schulte had lied about Amol's
21 behavior towards him?

22 A. Yes.

23 Q. And you were aware that Mr. Schulte was so upset by Amol's
24 behavior that he went to court, correct?

25 A. I was aware that he went to court. I don't know why he

K253SCH5

Weber - Cross

1 went to court.

2 Q. He didn't tell you he was upset?

3 A. I was not talking to him at this point.

4 Q. Okay. So, by then you had stopped talking to him?

5 A. Yes.

6 Q. Okay. But you were talking to Amol?

7 A. Yes.

8 Q. And Amol had gone to court with you?

9 A. Amol, I don't know -- at one point I went to court with

10 Amol. I don't know Amol's court appearances prior to that.

11 Q. Okay. So Amol told you the version of what Mr. Schulte was
12 doing?

13 A. Yes.

14 Q. And you believed Amol?

15 A. I saw what Amol had as well as the -- I read Mr. Schulte's
16 allegations.

17 Q. But you weren't talking to him?

18 A. No.

19 Q. So you heard what Amol said, and then you continued to side
20 with Amol?

21 A. Yes.

22 Q. Okay. Now, let me just move just very briefly for a second
23 from that to how the CIA maintained, as you called it, physical
24 security. Right.

25 A. Okay.

K253SCH5

Weber - Cross

1 Q. So you testified that to get into the CIA, physical
2 location, right, you had to have a badge, right?

3 A. That is the way that I would have accessed it. I had a
4 badge. Other people might not and would present like a
5 driver's license, and if they were on an access list, they
6 could, you know, access the facility.

7 Q. Okay. So when you access the CIA facility, do you drive
8 into like a big compound and then go to a building?

9 A. After you present your badge the first time, yes.

10 Q. Right. And then there's like a whole gigantic parking lot
11 or something like that where people park their cars?

12 A. Yes.

13 Q. Is there more than one physical building structure on that
14 lot?

15 A. Yes.

16 Q. How many physical structures are there?

17 A. The, at that time, I believe there was two. I don't know.
18 I don't know the status.

19 Q. Now, to go from one physical structure to another physical
20 structure, you didn't have to go through any additional driving
21 or security, correct?

22 A. Once you were inside the building, the two physical
23 structures I referenced were connected by a tunnel.

24 Q. So, once you got inside the building, you had CIA employees
25 inside the building, correct?

K253SCH5

Weber - Cross

1 A. Yes.

2 Q. You had people who contracted with the CIA and were
3 contractors, correct?

4 A. Yes.

5 Q. You had support staff and other staff who were part of the
6 CIA's workforce, correct?

7 A. That would fall into the one of the first two categories
8 you described.

9 Q. All told, how many people worked in that big area?

10 A. I have no idea the number. It was large.

11 Q. It was large, right?

12 A. Yes. It was a nine-floor building.

13 Q. So you would say over 1,000?

14 A. I don't know.

15 Q. You don't know. When you went from one building to another
16 building, you could carry with you documents, correct?

17 A. You were not leaving the secure portion of the facility, so
18 yes, that is correct.

19 Q. You could carry with you computers, correct?

20 A. Yes, that is correct.

21 Q. You could carry with you laptops, correct?

22 A. Yes.

23 Q. In fact, there were times when somebody moved from one
24 building to another, just physically carried their stuff with
25 them, correct?

K253SCH5

Weber - Cross

1 A. Yes. We were authorized to transport classified
2 information.

3 Q. Okay. When you worked at the CIA with Mr. Schulte, you
4 never saw Mr. Schulte walk off that garage or compound with a
5 hard drive, did you?

6 A. No.

7 Q. Did you ever see him walk off with a disc, did you?

8 A. No.

9 Q. How about a thumb drive? Did you see him walk off with a
10 thumb drive?

11 A. No.

12 Q. How about a computer? Did you see him walk off with a
13 computer?

14 A. No.

15 Q. When he worked at the CIA with you, did you ever see him
16 use a cell phone inside the facility?

17 A. No.

18 Q. And it's fair to say you would never do such a thing,
19 right?

20 A. Yes.

21 Q. Let's talk about systems security. Right. Because you
22 testified on direct with Mr. Laroche that you thought that the
23 DevLAN system was secure, right?

24 A. Yes.

25 Q. Is that still your testimony now?

K253SCH5

Weber - Cross

1 A. Yes.

2 Q. Correct me if I'm wrong on any one of these, okay?

3 CCI work product properly resided on the DevLAN
4 network; is that correct?

5 A. I'm sorry. CCI work product?

6 Q. Right.

7 A. Properly resided on the network. Yes?

8 I don't know if I fully understand the question.
9 Like, what's a work product?

10 Q. It's not a trick. I'm just asking if the work that group
11 did was on the DevLAN network?

12 A. So, CCI is the largest portion of the umbrella. There was
13 a subset of CCI's work product, the stuff that was made by AED,
14 that would have been on the network. Maybe some other stuff
15 from other groups, but it was focused on EDG's product. Not
16 necessarily CCI's.

17 Q. Is it fair to say that CCI --

18 Let me take one step back.

19 What is CIMC; do you know?

20 A. It is the group that is specifically focused on
21 investigating counterintelligence and counterespionage.

22 Q. You've told us about every other acronym. Tell us what
23 CIMC stands for.

24 A. CIMC is the Counter Intelligence Mission Center.

25 Q. And is it fair to say that the CCI did not work with CIMC

K253SCH5

Weber - Cross

1 to properly develop or deploy user activity monitoring?

2 A. That was outside my scope.

3 Q. Okay. Would you agree with me that the system lacked
4 robust server audit capability?

5 A. I don't know what type of auditing was on the servers.

6 Q. But you testified on direct that the servers were secure,
7 right?

8 A. I can talk to the Atlassian products. I can't talk to
9 every server that was on DevLAN.

10 Q. How about the ESXi server?

11 A. The OSB ESXi server, it had some level of auditing that we
12 felt there was a need for.

13 Q. You have to say that again.

14 A. The OSB ESXi server we had the default auditing enabled.
15 So, we felt that was good enough for the needs for that server.

16 Q. Good enough?

17 A. Yes.

18 Q. What does that mean, "good enough"?

19 A. There's different, different levels of information. As I
20 had stated, most of what was on the OSB server was, it was
21 non-production data. It was test VMs and things like that.

22 Q. So you didn't think it was that secure or that secret, so
23 it didn't have to have a robust server audit capability?

24 A. I -- we set it up to defend what we -- we set it up to a
25 point where I feel it was good enough.

K253SCH5

Weber - Cross

1 Q. I'm sorry. Is that the place from which all of this stuff
2 was stolen?

3 A. I don't know where all of this stuff was stolen from.

4 Q. Oh. Okay. All right. Let's try the next one.

5 Is it fair to say that the cyber weapons were not
6 compartmented?

7 A. Generally correct.

8 Q. What does that even mean? Can you help me out here?

9 A. There were cases where some of our cyber capabilities would
10 have been compartmented.

11 Q. What does that mean though? I'm sorry.

12 A. I apologize. Compartment is very strict handling for
13 specific scenarios. Very limited need-to-know access.

14 Q. Right. And the cyber weapon is what?

15 A. Sorry, say that again?

16 Q. What's a cyber weapon?

17 A. A cyber weapon would be a potential term for the type of
18 capabilities we make.

19 Q. What does that mean, "type of capabilities we make"?

20 A. We made cyber tools.

21 Q. Right.

22 A. If you want to refer to them as weapons, I would probably
23 disagree with that terminology. But, other people might agree
24 with it.

25 Q. Could you just give me one second?

K253SCH5

Weber - Cross

1 A. Sure.

2 (Counsel conferring)

3 Q. Let me just stick to my question, okay. I got distracted
4 for a minute. I apologize.

5 By cyber weapon you mean the tools that your unit
6 created, right?

7 A. Like I said, it could be a definition. It's not how I
8 would describe them.

9 Q. Well, let's just go with what you would describe it. You
10 would call it some kind of malware, right, you said?

11 A. That would be an industry term I think is accurate.

12 Q. By malware, you basically mean it's something that the
13 United States creates so they can go spy on a foreign
14 government, correct?

15 A. That's one of the scenarios that we created it for.

16 Q. Right. And basically, when we speak like this, like it's
17 the scenario we created for, just to simplify it because we
18 don't all work at the CIA.

19 A. Yes.

20 Q. Right. So, you create a tool because you want to know what
21 some other countries, say Iran or France or Germany or some
22 other country, is up to, correct?

23 A. Without identifying specific countries, that is a correct
24 statement.

25 Q. So, the people who develop these tools, they make up a tool

K253SCH5

Weber - Cross

1 so that it can be used to get information from a foreign
2 country that we want. But we don't want anybody to know we're
3 doing it, so we try and hide it.

4 That's what all of these people are doing at EDG?

5 A. Yes.

6 Q. That is what you call a cyber tool, a cyber weapon, a
7 malware tool, all of these fancy words are just for what I
8 described, correct?

9 A. Yes.

10 Q. Okay. Of course, nobody wants it to be tracked back to us,
11 because then nobody would talk to us, correct?

12 A. That is correct.

13 Q. Is it fair to say that the users on these servers that we
14 have, and that you talked about, shared system administrative
15 level passwords?

16 A. For some servers.

17 Q. Isn't that like a bad thing to do?

18 A. Depends on the scenario.

19 Q. Can you think of any good reason, from a security
20 perspective, I'm not talking about collaboration and getting
21 things done fast, which is why I think this was done. I'm just
22 talking from a security perspective, can you think of any
23 reason you would ever have users share a system at an
24 administrative level where the passwords are shared?

25 A. Yes.

K253SCH5

Weber - Cross

1 Q. From a security point of view?

2 A. Yes.

3 Q. Tell us why.

4 A. Your typical scenario would tend to be a backup account in
5 case, in case your connection with Active Directory or
6 something like that broke.

7 Q. If one person's connection broke, that means they could use
8 somebody's else's password?

9 A. It was supposed to be a backup password for in case there
10 was no longer the traditional ways of logging in.

11 Q. Okay. So if you, for example, were logged out, or locked
12 out, you could go to this shared system admin level, because at
13 one point you were admin, and you could take one of those
14 passwords and log on in, correct?

15 A. Yes.

16 Q. Okay. And could you just take any password?

17 A. No.

18 Q. So which password would you pick from all of these
19 passwords?

20 A. What passwords are you referring to?

21 Q. These shared system admin level password.

22 A. The ones that we discussed earlier?

23 Q. Yeah.

24 A. I don't know. What am I trying to do?

25 Q. All I'm asking you is, it isn't the best way to keep a

K253SCH5

Weber - Cross

1 network safe. Correct?

2 A. It is -- you want to ensure that people are logging in with
3 a unique user name and password as much as possible.

4 Q. Right. This defeats that, correct?

5 A. This would circumvent that.

6 Q. I'm sorry, he coughed. I couldn't hear you.

7 A. This would circumvent that.

8 Q. Right. There was another problem with the system in the
9 sense that there was no effective removable media control,
10 correct?

11 A. I can't comment to that.

12 Q. Well, let's see if we can try. You testified with
13 Mr. Laroche here that you were part of this recovery effort
14 after the leak, correct?

15 A. Yes.

16 Q. When was the first leak in your mind?

17 A. March 7.

18 Q. March 7. And when the March 7 leak came, did anybody at
19 the CIA say, hey, is this about it or is there more to come?

20 A. I -- I was not part of any conversations like that. It was
21 not my focus at the time.

22 Q. It was not your focus to see what else could be coming down
23 the turnpike, considering this was like the CIA's most precious
24 hacking tools?

25 A. My focus was on assessing what was in Confluence and what

K253SCH5

Weber - Cross

1 information we could take from Confluence.

2 Q. Okay. So when you first discovered that this had been put
3 on WikiLeaks, how long did it take, not you personally -- or
4 let's start with you personally.

5 How long did it take you to figure out that the stuff
6 was like a year old?

7 A. It would have been during that first week.

8 Q. It took a whole week to figure out it was a year old?

9 A. It wasn't something we were specifically trying to figure
10 out at the time.

11 Q. How many people were on your team?

12 A. Are you referencing the team during that first week?

13 Q. Yeah.

14 A. About 10 people.

15 Q. 10 people were on your team. Right?

16 A. Give or take.

17 Q. How many teams were there, all told?

18 A. During that first week, I think there might have been two
19 teams. I don't recall.

20 Q. On these two teams, it took a whole week to figure out that
21 the information you guys were talking about was a year old.

22 A. We were not looking for that information.

23 Q. You were trying to assess damage, right?

24 A. Yes.

25 Q. You were trying to assess damage of a leak, correct?

K253SCH5

Weber - Cross

1 A. Yes.

2 Q. You wanted to know what was leaked, correct?

3 A. Yes.

4 Q. And you wanted to know if that leak was going to hurt,
5 correct?

6 A. Yes.

7 Q. So the first thing you want to know is what is leaked,
8 correct?

9 A. What was leaked, yes.

10 Q. Right. What was leaked. And how recent is the
11 information. Right?

12 A. No.

13 Q. You didn't want to know how recent the information was?

14 A. I didn't necessarily care.

15 Q. You didn't care if the most recent tool had been leaked to
16 find out how recent the leak was?

17 A. I cared about what information was leaked. Not the date of
18 that information.

19 Q. Right. So when you were trying to figure out what
20 information was leaked, you learned a week later that the
21 information that was leaked was about a year old.

22 A. I learned during that first week.

23 MS. SHROFF: Would this be a good place to stop?

24 THE COURT: I was just going to ask you if this was a
25 convenient place to break.

K253SCH5

Weber - Cross

1 MS. SHROFF: This is a good place to break.

2 THE COURT: We are going to break now. And we'll
3 resume at 9 o'clock tomorrow morning.

4 Please remember my instructions. Don't do any
5 independent research, don't talk about the case. If you see
6 anything in the newspaper, hear anything on the radio, ignore
7 it. You've got to make up your minds when the case goes to
8 you, it's in your hands. You have to consider only the
9 evidence that is brought out in this courtroom, and nothing
10 else.

11 So, safe home tonight. See you tomorrow morning at
12 9 o'clock. We'll have coffee and tea for you at 8:30.

13 Thanks very much.

14 (Jury excused)

15 THE COURT: You're on cross-examination so don't talk
16 to the government's attorneys.

17 THE WITNESS: Understood.

18 THE COURT: See you tomorrow morning at 9 o'clock.

19 MR. LAROCHE: Thank you, your Honor.

20 (Adjourned to February 6, 2020, at 9:00 a.m.)
21
22
23
24
25

INDEX OF EXAMINATION

Examination of:	Page
-----------------	------

JEREMY WEBER

Direct By Mr. Laroche	166
---------------------------------	-----

Cross By Ms. Shroff	353
-------------------------------	-----

GOVERNMENT EXHIBITS

Exhibit No.	Received
-------------	----------

89	189
--------------	-----

3004, 100, 111, 200, 300, 500	200
---	-----

601-616, 701, 702, 704-708	200
--------------------------------------	-----

712-714, 716, 718, 719, 720	200
---------------------------------------	-----

1001-1012, 1015-1056, 1058-1098	200
---	-----

1100-1103, 1105, 1107, 1108	200
---------------------------------------	-----

1110-1116, 1118, 1119, 1121	200
---------------------------------------	-----

1124, 1128-1130, 1132-1137, 5001	201
--	-----

1251	215
----------------	-----

90	237
--------------	-----

3005, 1201-1212, and all exhibits contained therein	217
---	-----

801	335
---------------	-----

806	338
---------------	-----

809	339
---------------	-----